IEEE computer society

IT Professional
Technology Solutions for the Enterprise

Cybersecurity – Grid, IoT and Smart City

Cyberthreats and Security

Tim Weil – CISSP/CCSP, CISA, PMP
IEEE Senior Member

University of Denver
Denver, CO
Jul 24, 2019

VOLUME 20, NUMBER 3 MAY/JUNE 2018

Cyberthreats and Security

Objectives of this Presentation

Cyberthreats and Security

-- The Changing Landscape (2015 v 2018)

-- Information Security – A body of knowledge

Grid Cybersecurity Resilience (Ukraine)

-- Advanced Persistent Threats (APT)

-- Cyber Attack Strategy

-- Industrial Control Systems (ICS) Kill Chain

-- Remediation Defenses (Passive, Active, Architecture))

Mirai Distributed Denial of Service – IoT Security

-- IoT Landscape

-- Mirai DDoS IoT Attack (Oct 2016)

-- Internet of Things (IoT) Forensics

-- How Mirai Works

-- Remediations and the CSA IoT Security Guidelines

Security and Privacy for the Smart City

-- Computer Society Publications

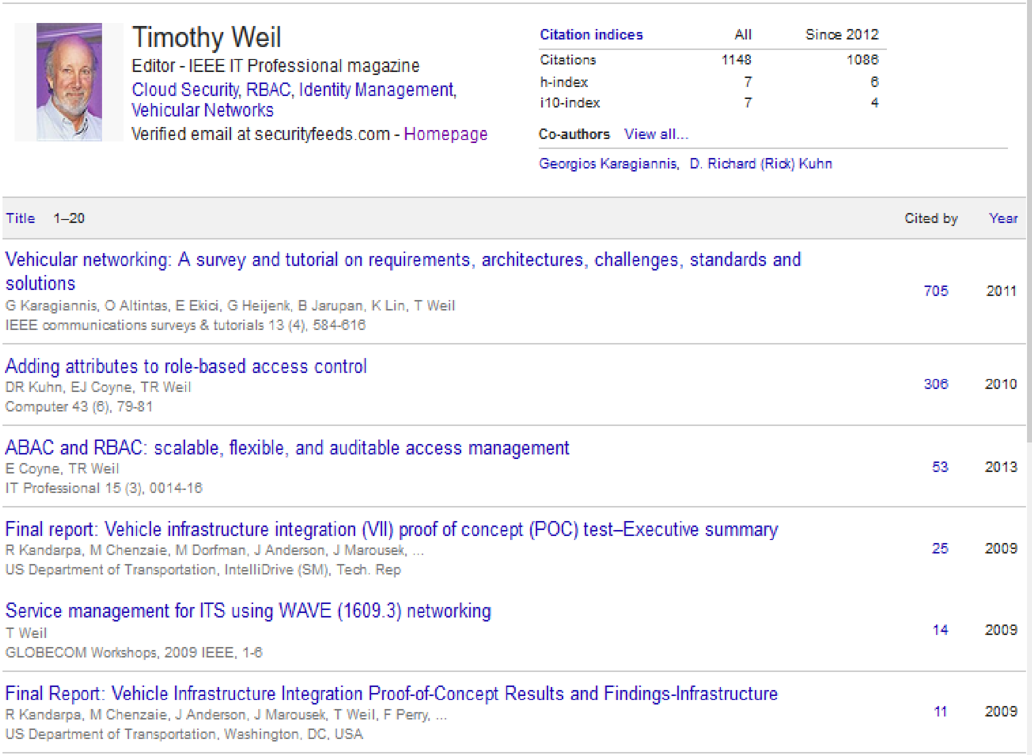
-- The Write Stuff

-- Author’s Portal

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- Security and Privacy of Smart Cities
- References + Q&A

A Writer’s Life –



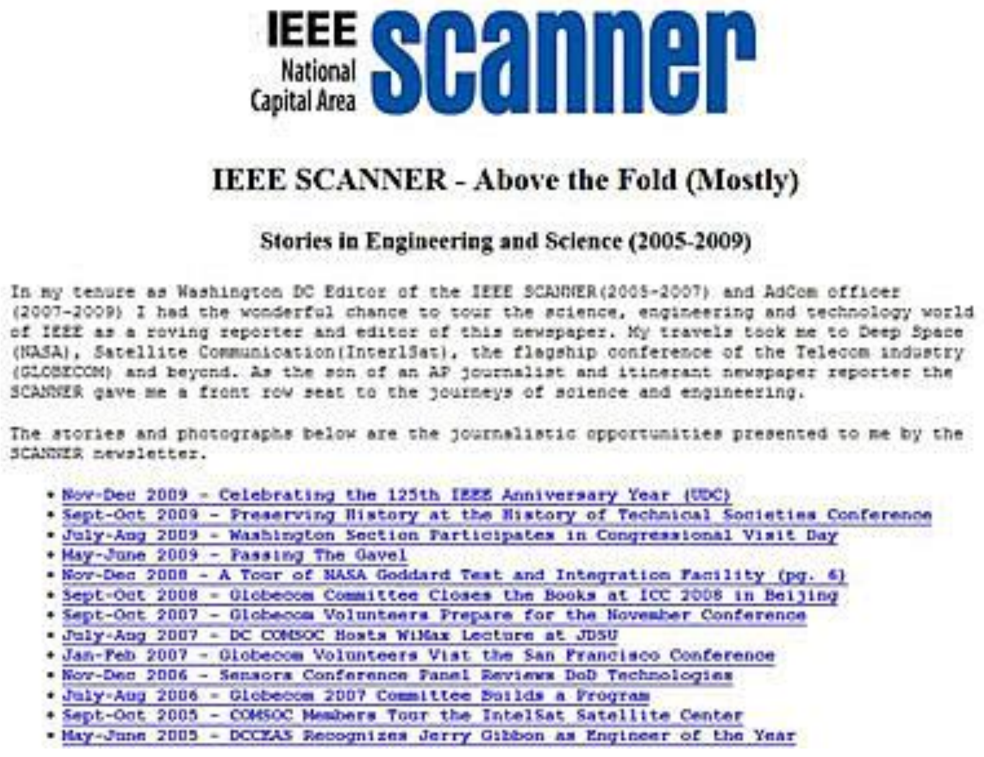
Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...

Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ... US Department of Transportation, Washington, DC, USA	11	2009



IEEE National Capital Area scanner

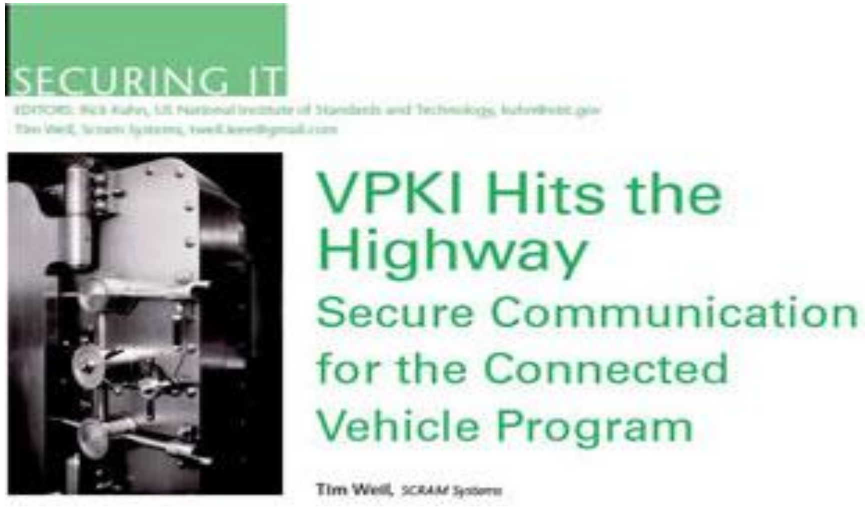
IEEE SCANNER - Above the Fold (Mostly)

Stories in Engineering and Science (2005-2009)

In my tenure as Washington DC Editor of the IEEE SCANNER(2005-2007) and AdCom officer (2007-2009) I had the wonderful chance to tour the science, engineering and technology world of IEEE as a roving reporter and editor of this newspaper. My travels took me to Deep Space (NASA), Satellite Communication(InterlSat), the flagship conference of the Telecom industry (GLOBECOM) and beyond. As the son of an AP journalist and itinerant newspaper reporter the SCANNER gave me a front row seat to the journeys of science and engineering.

The stories and photographs below are the journalistic opportunities presented to me by the SCANNER newsletter.

- Nov-Dec 2009 - Celebrating the 125th IEEE Anniversary Year (UDC)
- Sept-Oct 2009 - Preserving History at the History of Technical Societies Conference
- July-Aug 2009 - Washington Section Participates in Congressional Visit Day
- May-June 2009 - Passing The Gavel
- Nov-Dec 2008 - A Tour of NASA Goddard Test and Integration Facility (pg. 6)
- Sept-Oct 2008 - Globecom Committee Closes the Books at ICC 2008 in Beijing
- Sept-Oct 2007 - Globecom Volunteers Prepare for the November Conference
- July-Aug 2007 - DC COMSOC Hosts WiMax Lecture at JDSU
- Jan-Feb 2007 - Globecom Volunteers Vist the San Francisco Conference
- Nov-Dec 2006 - Sensors Conference Panel Reviews DoD Technologies
- July-Aug 2006 - Globecom 2007 Committee Builds a Program
- Sept-Oct 2005 - COMSOC Members Tour the IntelSat Satellite Center
- May-June 2005 - DCCEAS Recognizes Jerry Gibbon as Engineer of the Year



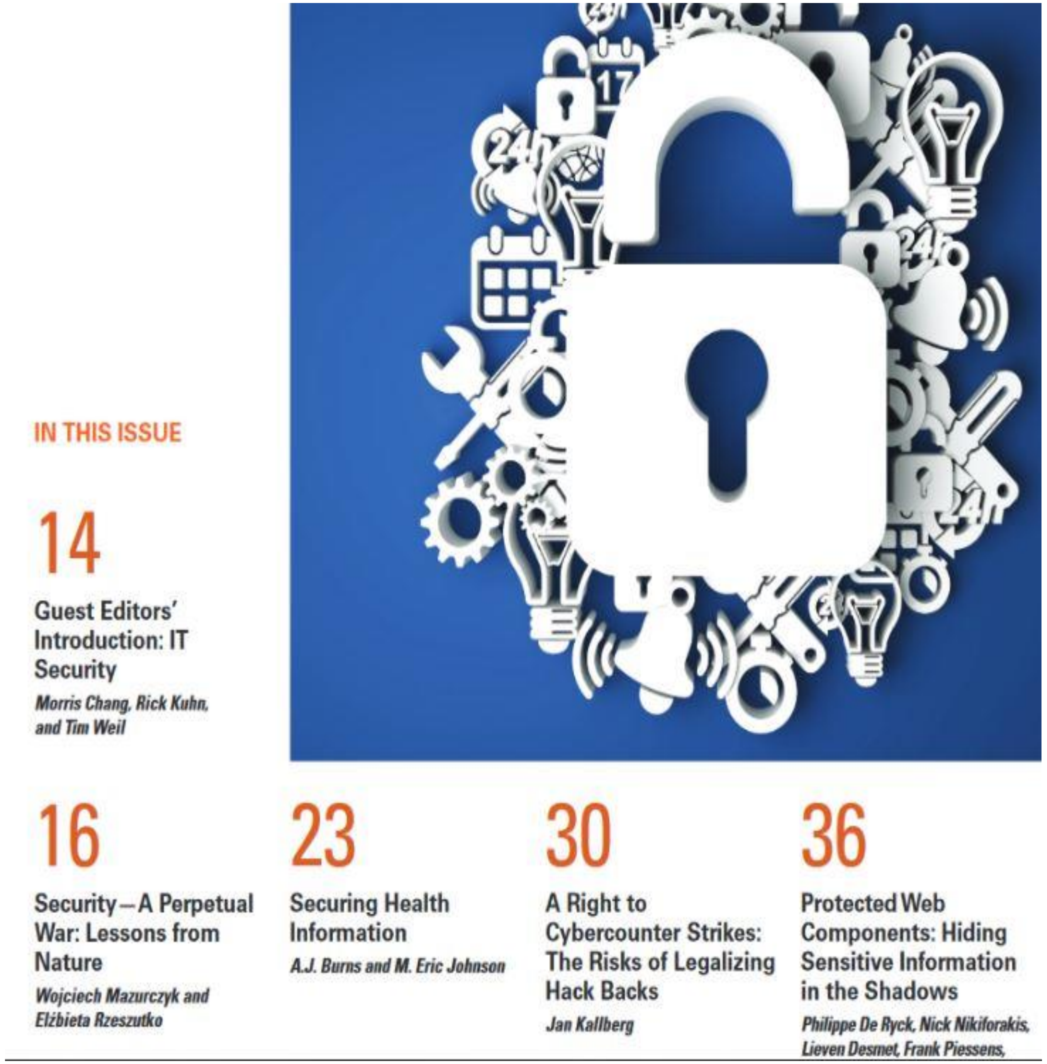
SECURING IT

EDITORS: Rick Kuhn, US National Institute of Standards and Technology, kuhn@nist.gov
Tim Weil, Scram Systems, tweil.ieee@gmail.com

VPKI Hits the Highway
Secure Communication for the Connected Vehicle Program

Tim Weil, SCRAM Systems

IT Professional Security Issue (2015 vs 2018)



IN THIS ISSUE

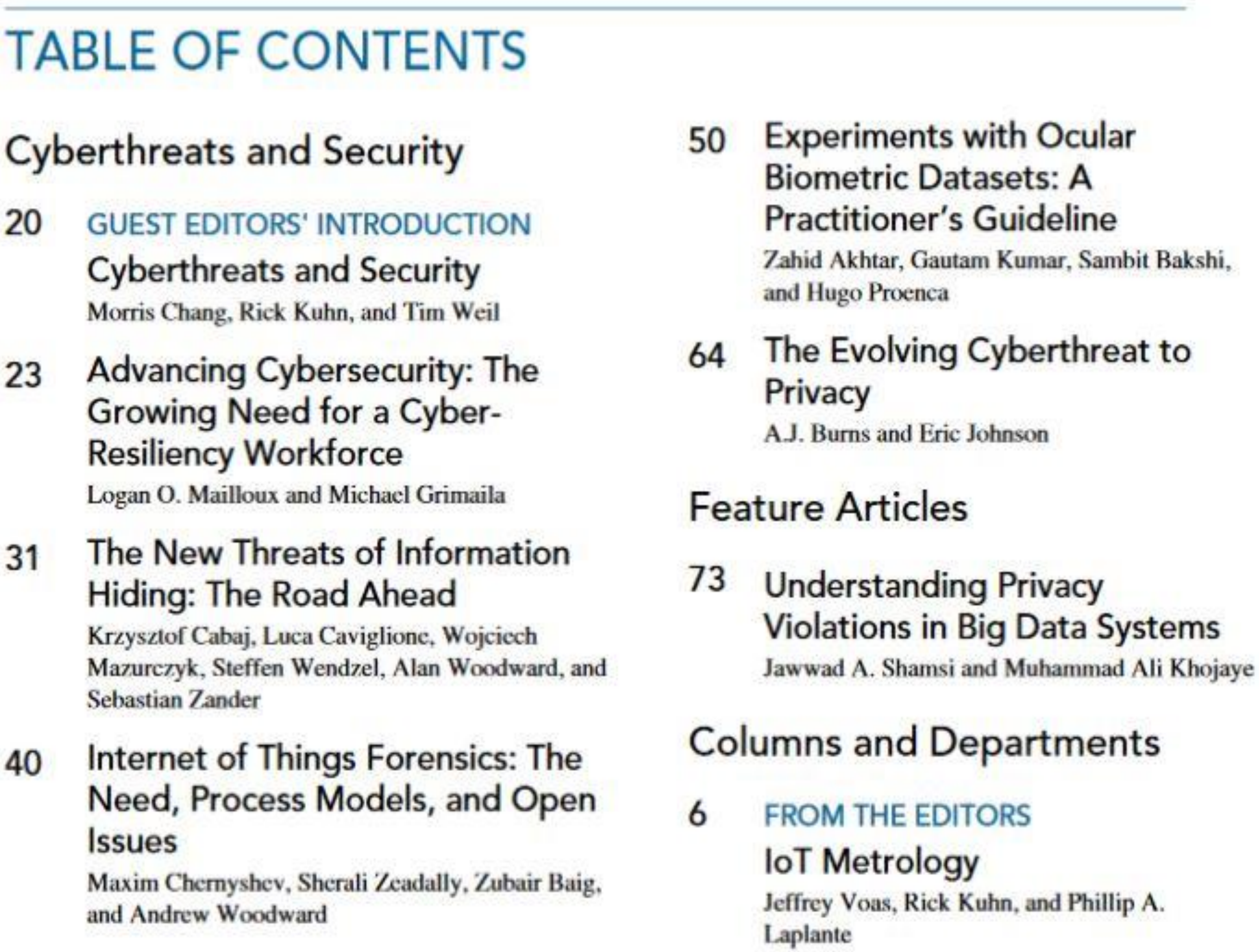


TABLE OF CONTENTS

Cyberthreats and Security

Feature Articles

Columns and Departments

A Cybersecurity Body of Knowledge – IEEE Security and Privacy (May/June 2018)

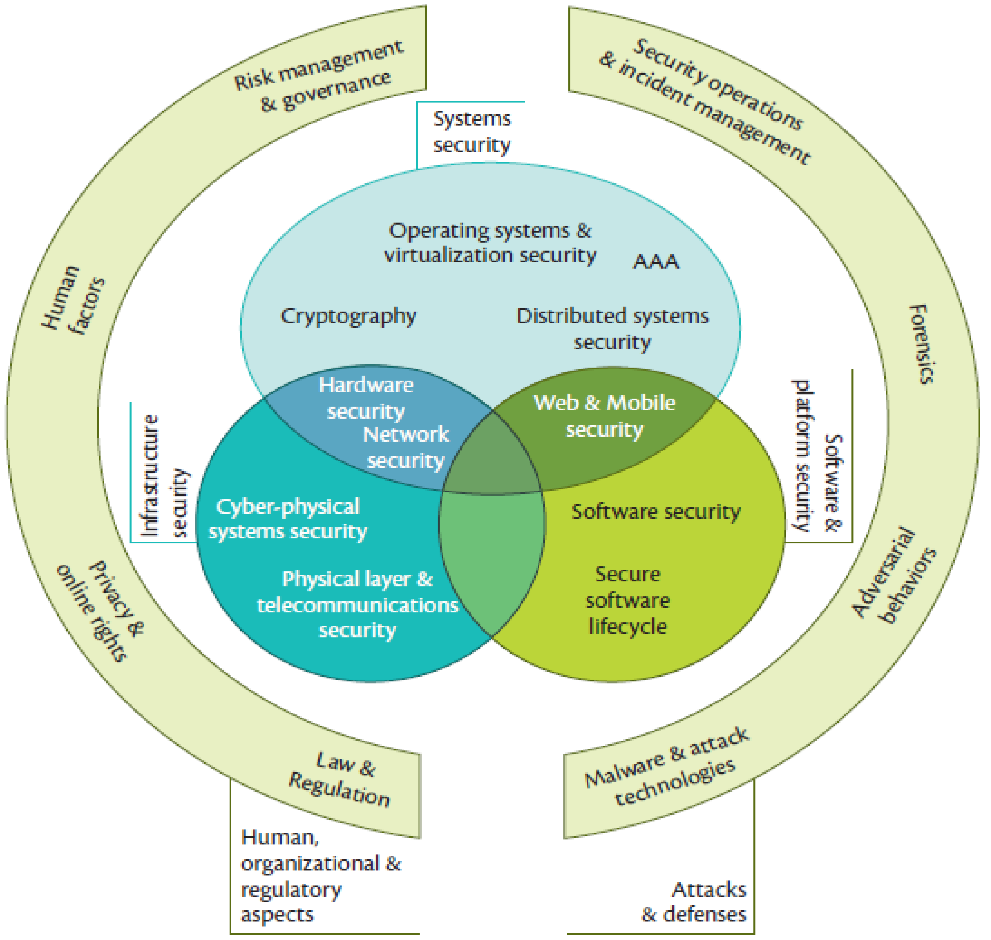

Risk management & governance
Security operations & incident management
Systems security
Operating systems & virtualization security
AAA
Cryptography
Distributed systems security
Human factors
Forensics
Hardware security
Network security
Web & Mobile security
Software & platform security
Infrastructure security
Cyber-physical systems security
Software security
Physical layer & telecommunications security
Secure software lifecycle
Privacy & online rights
Adversarial behaviors
Law & Regulation
Malware & attack technologies
Human, organizational & regulatory aspects
Attacks & defenses

Figure 3. The 19 knowledge areas and their categorization within CyBOK.

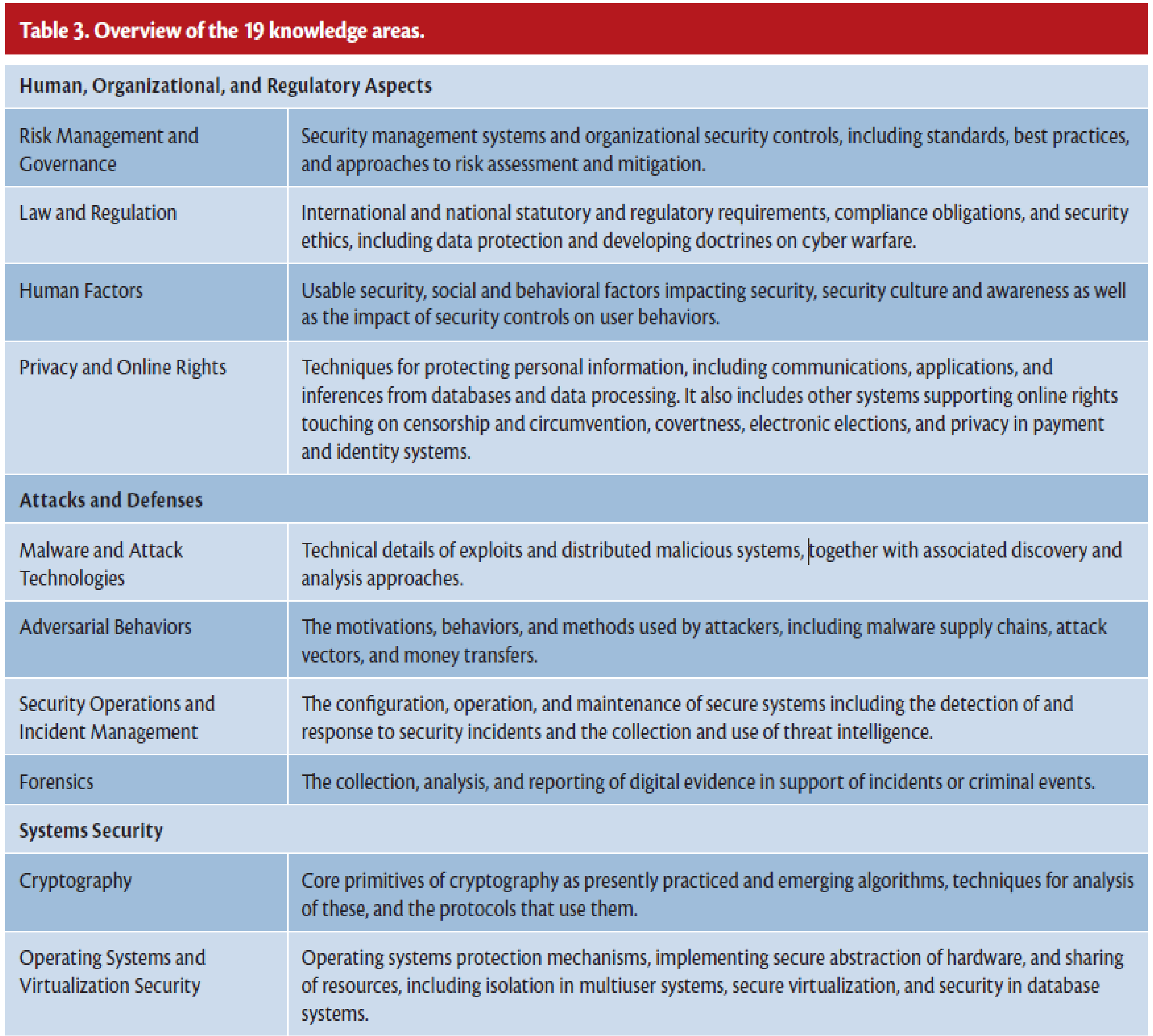


Table 3. Overview of the 19 knowledge areas.

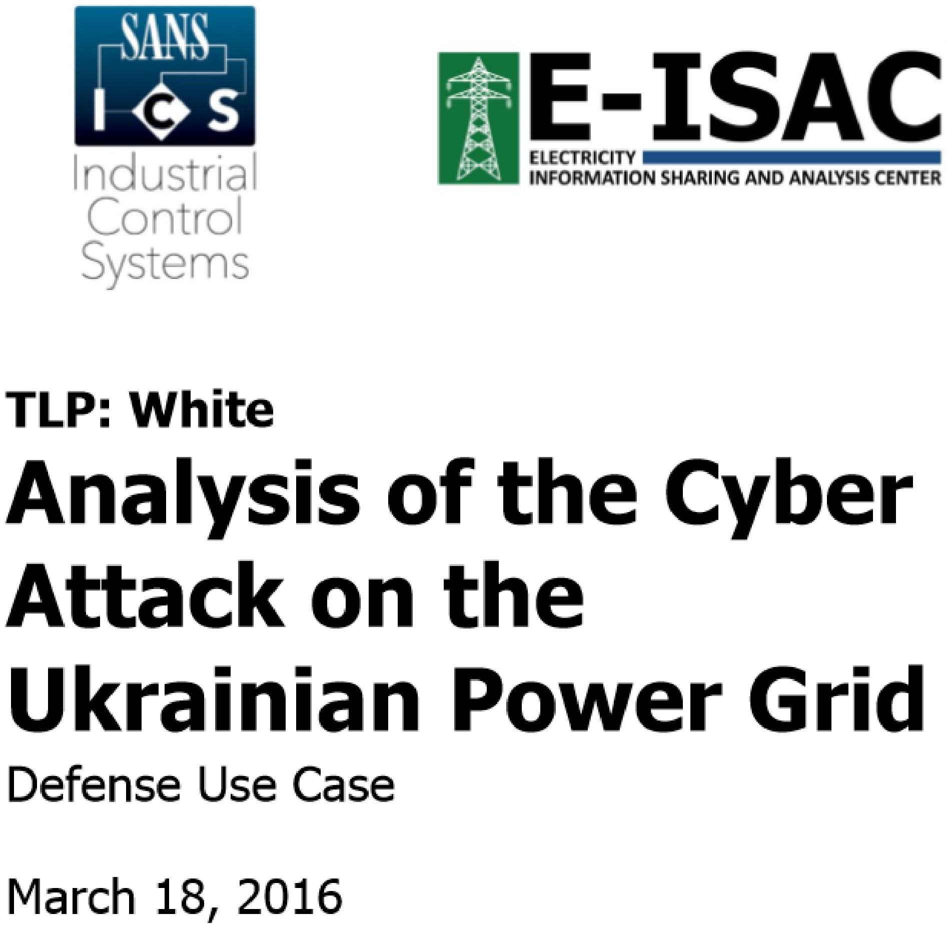
Human, Organizational, and Regulatory Aspects	
Risk Management and Governance	Security management systems and organizational security controls, including standards, best practices, and approaches to risk assessment and mitigation.
Law and Regulation	International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines on cyber warfare.
Human Factors	Usable security, social and behavioral factors impacting security, security culture and awareness as well as the impact of security controls on user behaviors.
Privacy and Online Rights	Techniques for protecting personal information, including communications, applications, and inferences from databases and data processing. It also includes other systems supporting online rights touching on censorship and circumvention, covertness, electronic elections, and privacy in payment and identity systems.
Attacks and Defenses	
Malware and Attack Technologies	Technical details of exploits and distributed malicious systems, together with associated discovery and analysis approaches.
Adversarial Behaviors	The motivations, behaviors, and methods used by attackers, including malware supply chains, attack vectors, and money transfers.
Security Operations and Incident Management	The configuration, operation, and maintenance of secure systems including the detection of and response to security incidents and the collection and use of threat intelligence.
Forensics	The collection, analysis, and reporting of digital evidence in support of incidents or criminal events.
Systems Security	
Cryptography	Core primitives of cryptography as presently practiced and emerging algorithms, techniques for analysis of these, and the protocols that use them.
Operating Systems and Virtualization Security	Operating systems protection mechanisms, implementing secure abstraction of hardware, and sharing of resources, including isolation in multiuser systems, secure virtualization, and security in database systems.

“Scoping the Cyber Security Body of Knowledge” Awais Rashid, et. al

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- Security and Privacy of Smart Cities
- References + Q&A

Grid Cybersecurity in the News



SANS ICS Industrial Control Systems

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

TLP: White

Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

March 18, 2016

https://www.forbes.com/sites/kateoflahertyuk/2019/07/03/u-s-government-makes-surprise-move-to-secure-power-grid-from-cyber-attacks/#46ecff7a3191

On December 23, 2015, the control centers of three Ukrainian electricity distribution companies were remotely accessed. Taking control of the facilities' SCADA systems, malicious actors opened breakers at some 30 distribution substations in the capital city Kiev and western Ivano-Frankivsk region, causing more than 200,000 consumers to lose power Nearly a year later, on December 17, 2016, a single transmission substation in northern Kiev lost power. These instances of sabotage took place on the tail of a political revolution in Kiev, the annexation of Crimea, and amid military clashes in the eastern Donetsk and Luhansk regions.

A Decade of Energy Cyber Infrastructure Attack Malware

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

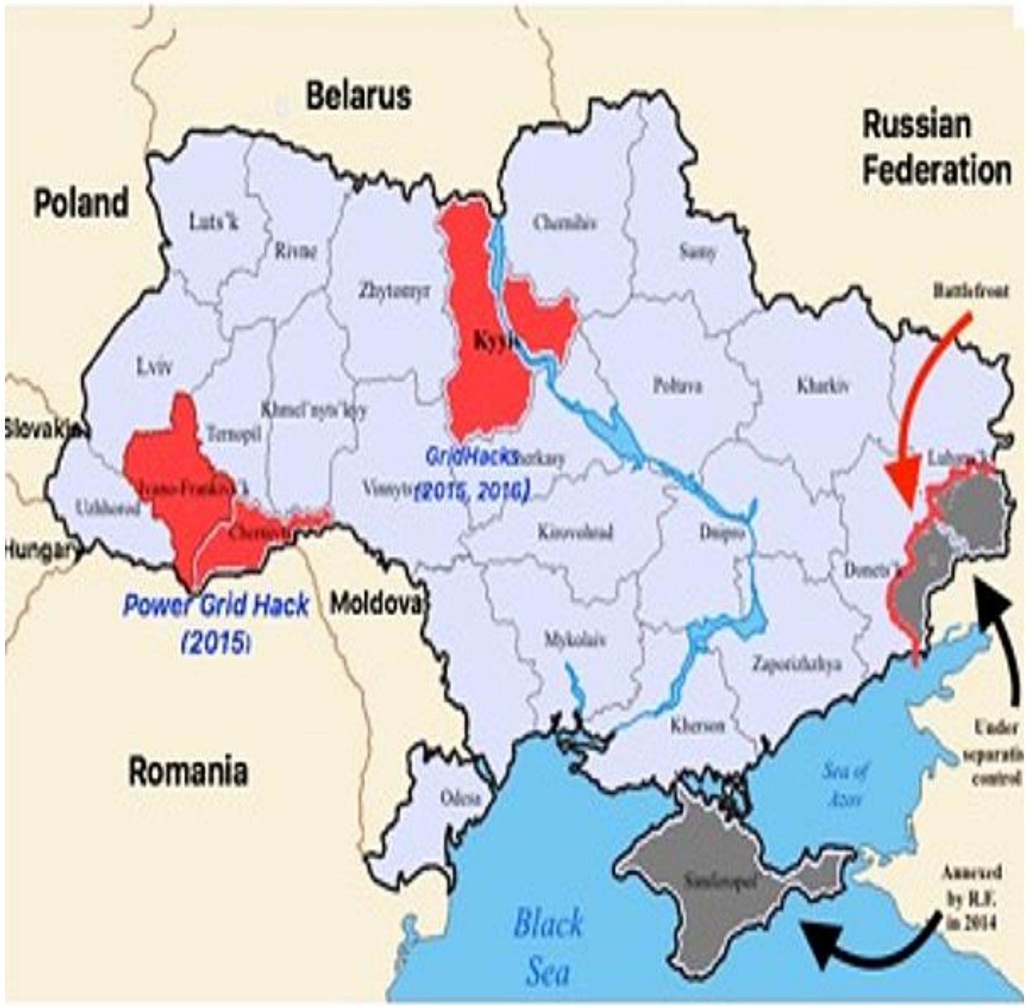
- **2010: Stuxnet:** Targeted Siemans industrial control systems in Iran. Was first discovered malware that spies on and subverts industrial systems and the first to include a programmable logic controller (PLC) rootkit.
- **2014: Dragonfly/Havex:** Focus was to collect ICS network and access control information. Evidence suggests this was provided to a well organized and funded group outside countries from which the data was collected.
- **2015: Black Energy 3:** Used in attack on the Ukraine power grid. Considered to be the first known power grid cyberattack. Hackers were able to successfully compromise information systems of three energy distribution companies and temporarily disrupt electricity supply to the end consumers.
- **2016: CRASHOVERRIDE:** Second known attack in Ukraine. Impacted a single transmission level substation. Significant increase in sophistication of attack code relative to past attacks.
- **2017: TRISIS/TRITON:** Incident at a critical infrastructure organization which targeted Schneider Electric's Triconex safety instrumented system (SIS) and where an attacker deployed malware which targeted systems provided emergency shutdown capability for industrial processes. Deployed against at least one victim in the Middle East.

Ukrainian Shale Deposits and Russian Electrical Grid Attacks

The discovery of shale deposits has prompted Russian attempts to stall their developments and sabotage much needed business deals for Ukraine's foreign capital thirsty economy. Russia's military operation on the ground solved the prospects of Ukrainian energy competition problem for Russia, albeit *partially*.[83] The warzone in the Eastern Ukraine covers the Donetsk region part of Yuzivska shale bloc, and, thus, closed it to development.

In addition, the Kharkiv region (second half of the shale bloc) has been subject to destabilizing activities. Among these actions were the recent explosions at an arms warehouse in Balaklia, in the Kharkiv region, which, according to Ukraine's defense minister Poltorak, was staged by Russia.[84] It is also worth noting that at the beginning of the unrest in the Eastern Ukraine, there were numerous attempts, however unsuccessful, to create Russia-backed third separatist enclave in Kharkiv region.[85]

To prevent the development of energy sources in Ukraine's west, Moscow has employed various methods to destabilize the region – including attacks on the electrical grid. On December 23, 2015, Russian-led cyberattack on the Prykarpattyaoblenergo distribution center created enough uncertainty to hurt the prospects of setting up industrial fracking operations in that region. Ivano-Frankivsk region that hosts part of Olesska's shale block. Russian has also financed fracking protests The map illustrates the locations of the major attacks on the electrical grid



Ukraine Grid Utility Cybersecurity Attack – FireEye

https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf

In the first publicly documented power outage attributed to a cyber attack, Russian-nexus actors caused blackouts in several regions in Ukraine. The actors used spear phishing to plant BlackEnergy3 malware, which was used to disable control system computer. Responders also found a wiper module called killdisk that was used to disable both control and non-control systems computers. At the same time, the attackers overwhelmed utility call centers with automated telephone calls, impacting the utilities' ability to receive outage reports from customers and frustrating the response effort.

While killdisk does not have the functionality to open breakers – which would cause the outages – it would impede utility visibility of breaker status, and inhibit remote control of the substations. This suggests that the attackers used another method to cause the power outage, perhaps using interactive access via compromised corporate and SCADA accounts to remotely open individual breakers or initiate load shedding, sending simultaneous trip commands to multiple breakers.

Who is behind this attack?

BlackEnergy is a Trojan that was created by a hacker known as Cr4sh. In 2007, he reportedly stopped working on it and sold the source code for an estimated $700. The source code appears to have been picked by one or more threat actors and was used to conduct DDoS attacks against Georgia in 2008. These unknown actors continued launching DDoS attacks over the next few years. Around 2014, a specific user group of BlackEnergy attackers came to our attention when they began deploying SCADA-related plugins to victims in the ICS and energy sectors around the world

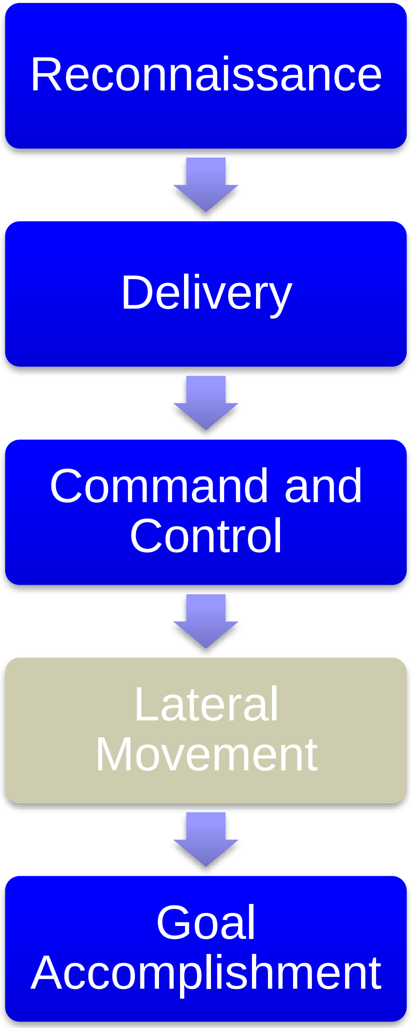
Potential Power-System-Specific Cyber Attack Strategies

http://www.aaes.org/sites/default/files/Sanders_Convocation2018.pdf

- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Corrupting Control Information: Smart Meters, SCADA Data, PMU Data, Dispatch Information, etc.
- Sophisticated lateral movement attacks
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

Lateral Movement in Cyber Kill Chain Demands Resiliency

http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf



Reconnaissance

- Port scanning
- Media analysis

Delivery

- Spear phishing
- Zero-day exploits

Command and Control

- Control channels

Lateral Movement

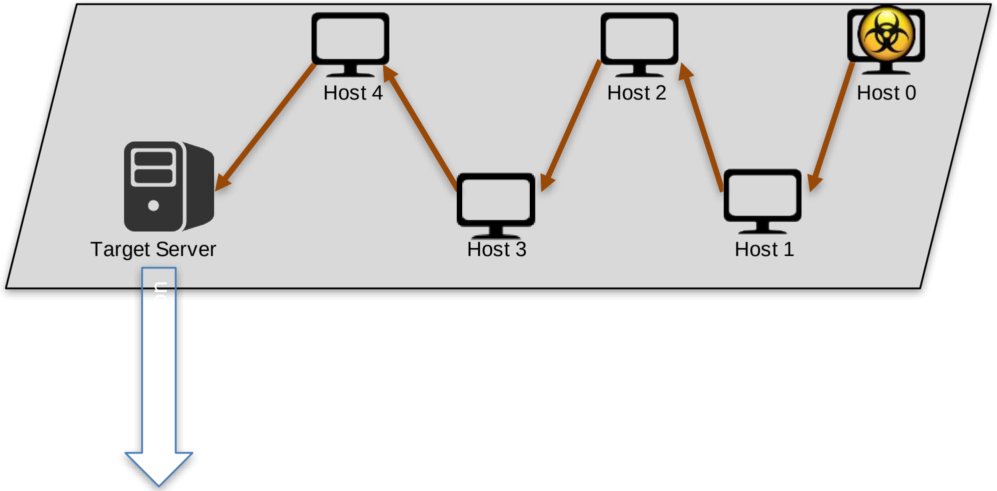
- Remote desktop
- Privilege escalation

Goal Accomplishment

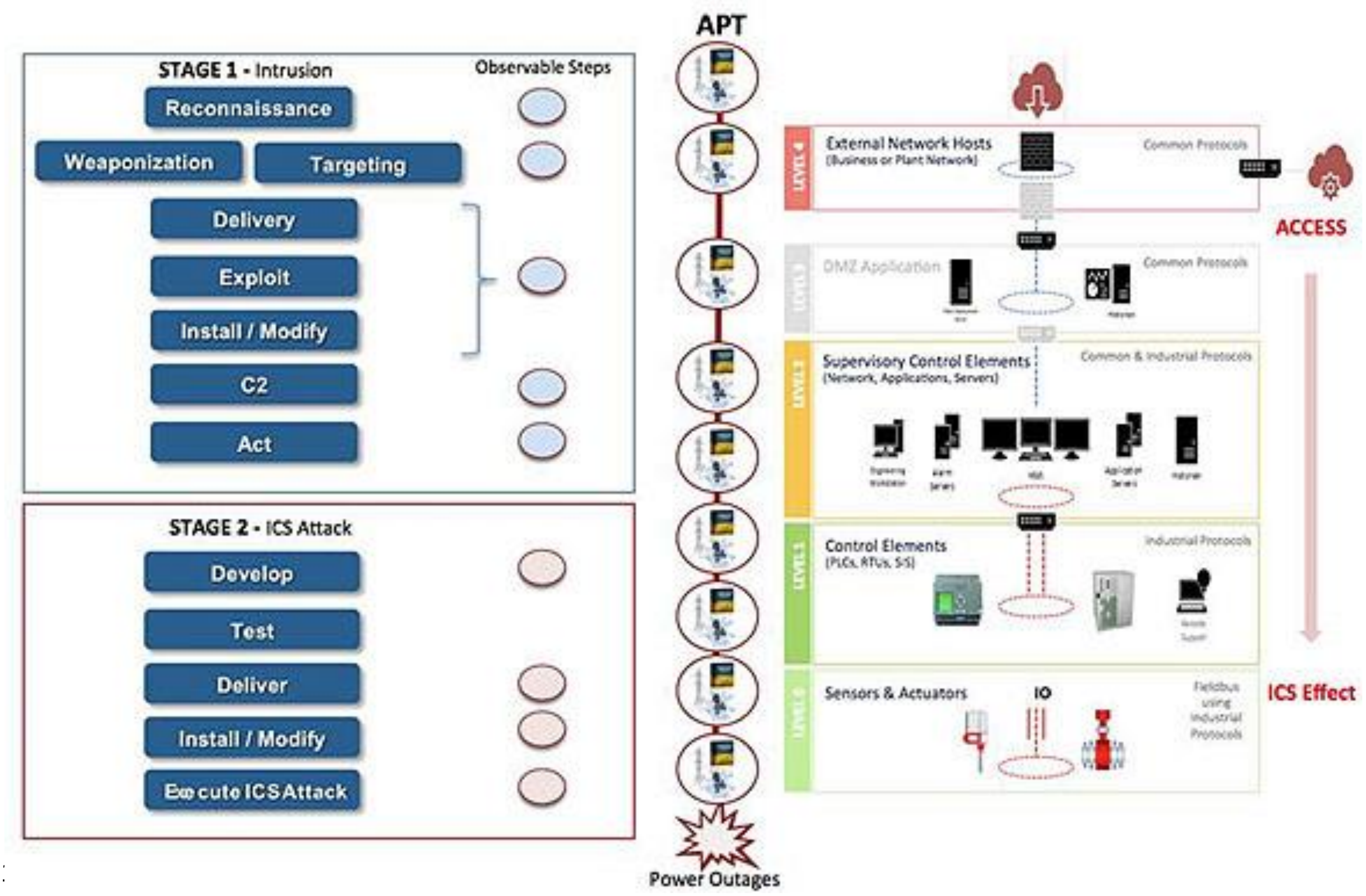
- Data exfiltration
- Physical damage

<u>During lateral movement:</u>

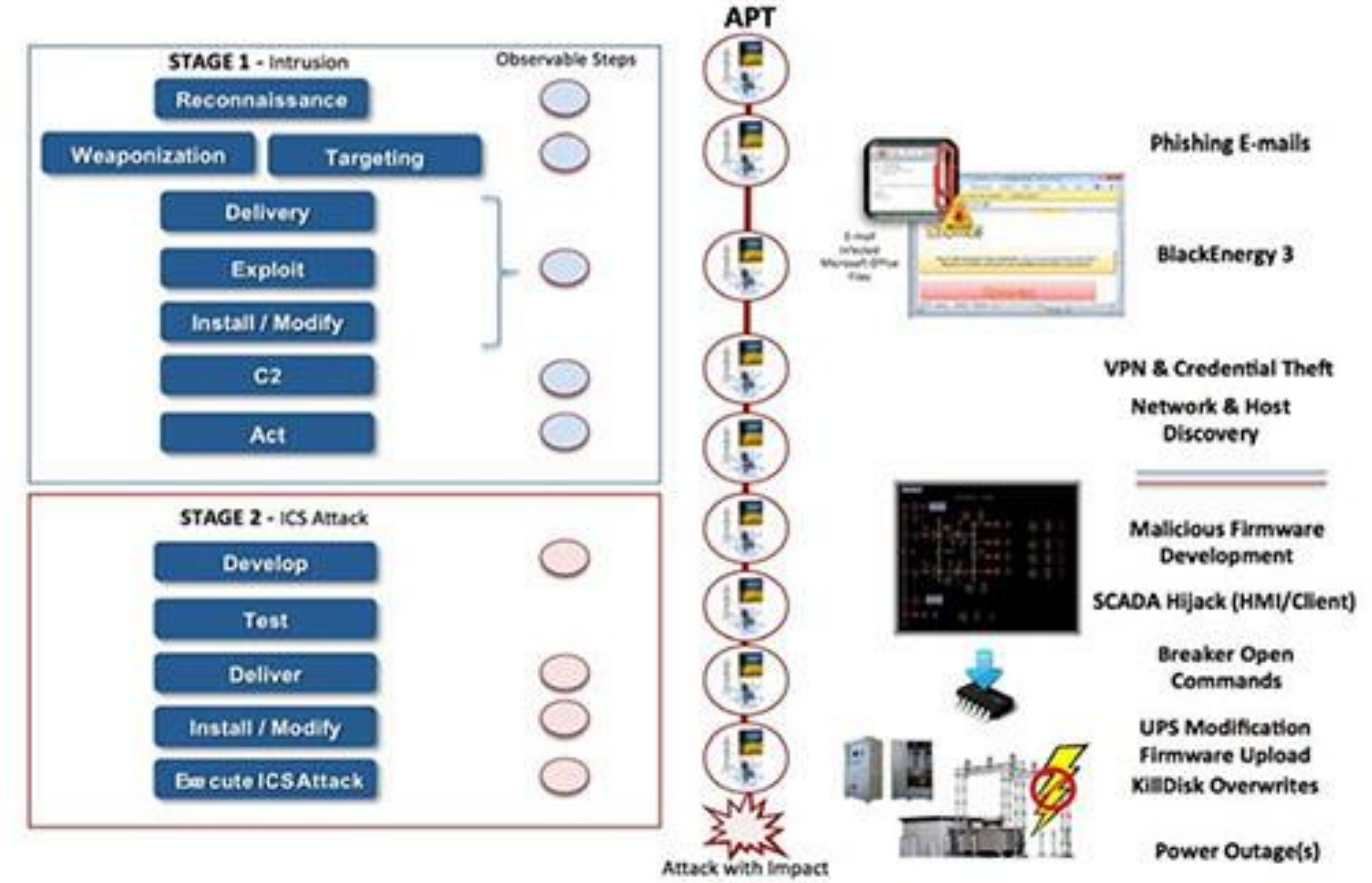
- Attacker moves laterally between hosts
- Attacker uses remote desktop connections, SSH, Windows management inventory, administrator tools



Ukraine Cyber Attack ICS Kill Chain (1 of 2)

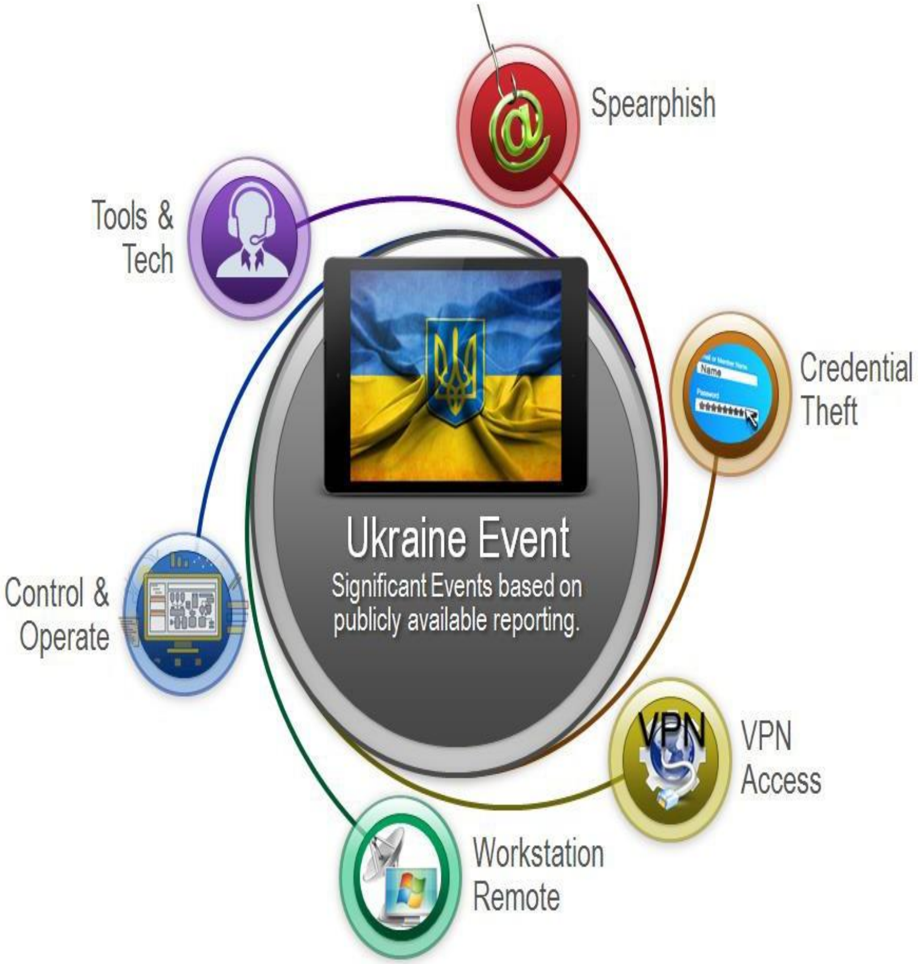


Ukraine Cyber Attack ICS Kill Chain (2 of 2)



Ukraine Attack Consolidated Technical Components

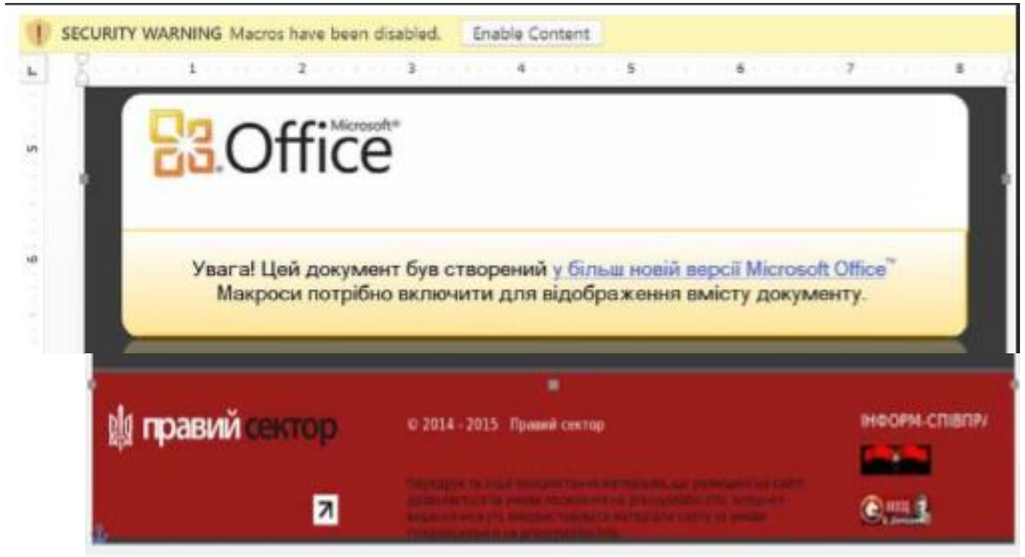
1. Spear phishing to gain access to the business networks of the
2. oblenergos
3. Identification of BlackEnergy 3 at each of the impacted oblenergos
4. Theft of credentials from the business networks
5. The use of virtual private networks (VPNs) to enter the ICS network
6. The use of existing remote access tools within the environment or issuing commands directly from a remote station similar to an operator HMI
6. Serial-to-ethernet communications devices impacted at a firmware level
7. The use of a modified KillDisk to erase the master boot record of impacted organizationsystems as well as the targeted deletion of some logs
8. Utilizing UPS systems to impact connected load with a scheduled service outage
9. Telephone denial-of-service attack on the call center



Ukraine Attack – Black Energy Malware (APT 1 of 2) -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During the cyber intrusion stage of **Delivery, Exploit, and Install**, the malicious Office documents were delivered via email to individuals in the administrative or IT network of the electricity companies. When these documents were opened, a popup was displayed to users to encourage them to enable the macros in the document as shown in Figure. Enabling the macros allowed the malware to Exploit Office macro functionality to install BlackEnergy 3 on the victim system and was not an exploit of a vulnerability through exploit code.


SECURITY WARNING Macros have been disabled.

Увага! Цей документ був створений у більш новій версії Microsoft Office™
Макроси потрібно включити для відображення вмісту документу.

Figure 6: A Sample of a BlackEnergy 3 Infected Microsoft Office Document[27]

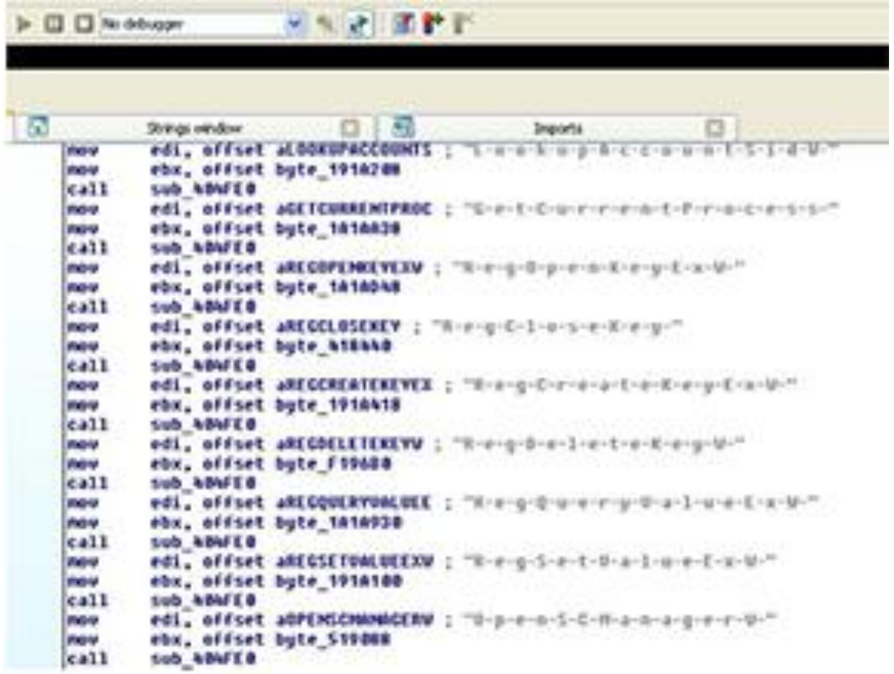
Upon the **Install** step, the BlackEnergy 3 malware connected to command and control (C2) IP addresses to enable communication by the adversary with the malware and the infected systems. These pathways allowed the adversary to gather information from the environment and enable access. The attackers appear to have gained access more than six months prior to December 23, 2015, when the power outage occurred. One of their first actions happened when the network was to harvest credentials, escalate privileges, and move laterally throughout the environment (e.g., target directory service infrastructure to directly manipulate and control the authentication and authorization system). At this point, the adversary completed all actions to establish persistent access to the targets.

Ukraine Attack – Kill Disk Malware -

https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

During **the ICS Attack Stage**, the adversaries used native software to Deliver themselves into the environment for direct interaction with the ICS components. They achieved this using existing remote administration tools on the operator workstations. The threat actors also continued to use the VPN access into the IT environment.

In final preparation for the attack, the adversaries completed the **Install/Mo**dify stage by installing malicious software identified as a modified or customized KillDisk across the environment. While it is likely the attackers then ensured their modifications to the UPS were ready for the attack, there was not sufficient forensic evidence available to prove this. The last act of modification was for the adversaries to take control of the operator workstations and thereby lock the operators out of their systems. Figure shows the static analysis of the KillDisk API imports following the event

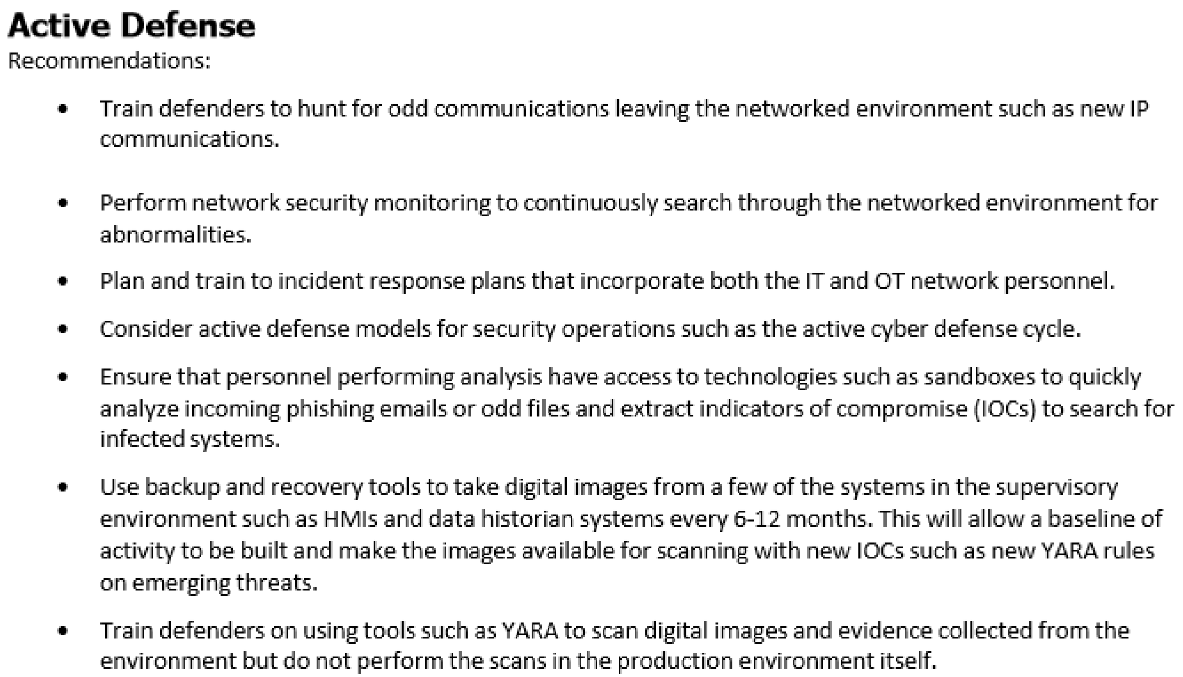


```
mov     edi, offset aLOOKUPACCOUNTS ; "L-o-o-k-u-p-A-c-c-o-u-n-t-S-i-d-W-"
mov     ebx, offset byte_1914200
call    sub_40WFE0
mov     edi, offset aGETCURRENTPROC ; "G-e-t-C-u-r-r-e-n-t-P-r-o-c-e-s-s-"
mov     ebx, offset byte_1914A30
call    sub_40WFE0
mov     edi, offset aREGOPENKEYEXW ; "R-e-g-O-p-e-n-K-e-y-E-x-W-"
mov     ebx, offset byte_1914048
call    sub_40WFE0
mov     edi, offset aREGCLOSEKEY ; "R-e-g-C-l-o-s-e-K-e-y-"
mov     ebx, offset byte_410440
call    sub_40WFE0
mov     edi, offset aREGCREATEKEYEX ; "R-e-g-C-r-e-a-t-e-K-e-y-E-x-W-"
mov     ebx, offset byte_1914418
call    sub_40WFE0
mov     edi, offset aREGDELETEKEYW ; "R-e-g-D-e-l-e-t-e-K-e-y-W-"
mov     ebx, offset byte_F19680
call    sub_40WFE0
mov     edi, offset aREGQUERYVALUEE ; "R-e-g-Q-u-e-r-y-V-a-l-u-e-E-x-W-"
mov     ebx, offset byte_1914930
call    sub_40WFE0
mov     edi, offset aREGSETVALUEEXW ; "R-e-g-S-e-t-V-a-l-u-e-E-x-W-"
mov     ebx, offset byte_1914100
call    sub_40WFE0
mov     edi, offset aOPENSCMANAGERW ; "O-p-e-n-S-C-M-a-n-a-g-e-r-W-"
mov     ebx, offset byte_519008
call    sub_40WFE0
```

Figure 7: Static Analysis of KillDisk Identifying API Imports[32]

Finally, to complete the ICS Cyber Kill Chain and to Execute the ICS Attack, the adversaries used the HMIs in the SCADA environment to open the breakers. At least 27 substations (the total number is probably higher) were taken offline across the three energy companies, impacting roughly 225,000 customers. Simultaneously, the attackers uploaded the malicious firmware to the serial-to-ethernet gateway devices. This ensured that even if the operator workstations were recovered, remote commands could not be issued to bring the substations back online

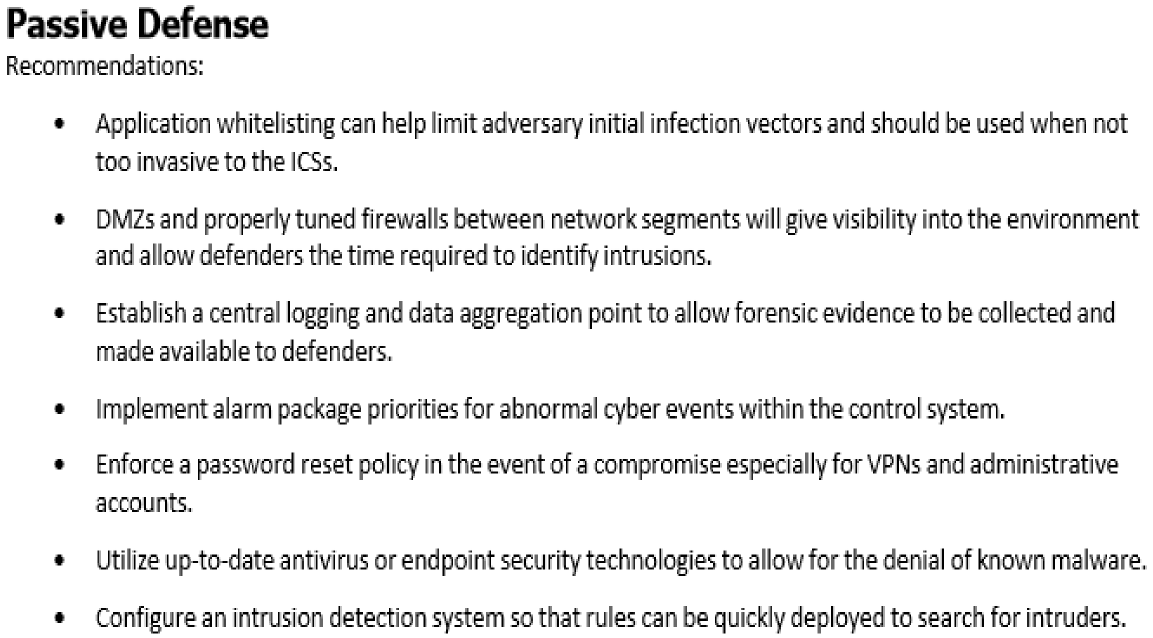
Ukraine Grid Attack – Remediation Defenses



Active Defense

Recommendations:

- Train defenders to hunt for odd communications leaving the networked environment such as new IP communications.
- Perform network security monitoring to continuously search through the networked environment for abnormalities.
- Plan and train to incident response plans that incorporate both the IT and OT network personnel.
- Consider active defense models for security operations such as the active cyber defense cycle.
- Ensure that personnel performing analysis have access to technologies such as sandboxes to quickly analyze incoming phishing emails or odd files and extract indicators of compromise (IOCs) to search for infected systems.
- Use backup and recovery tools to take digital images from a few of the systems in the supervisory environment such as HMIs and data historian systems every 6-12 months. This will allow a baseline of activity to be built and make the images available for scanning with new IOCs such as new YARA rules on emerging threats.
- Train defenders on using tools such as YARA to scan digital images and evidence collected from the environment but do not perform the scans in the production environment itself.



Passive Defense

Recommendations:

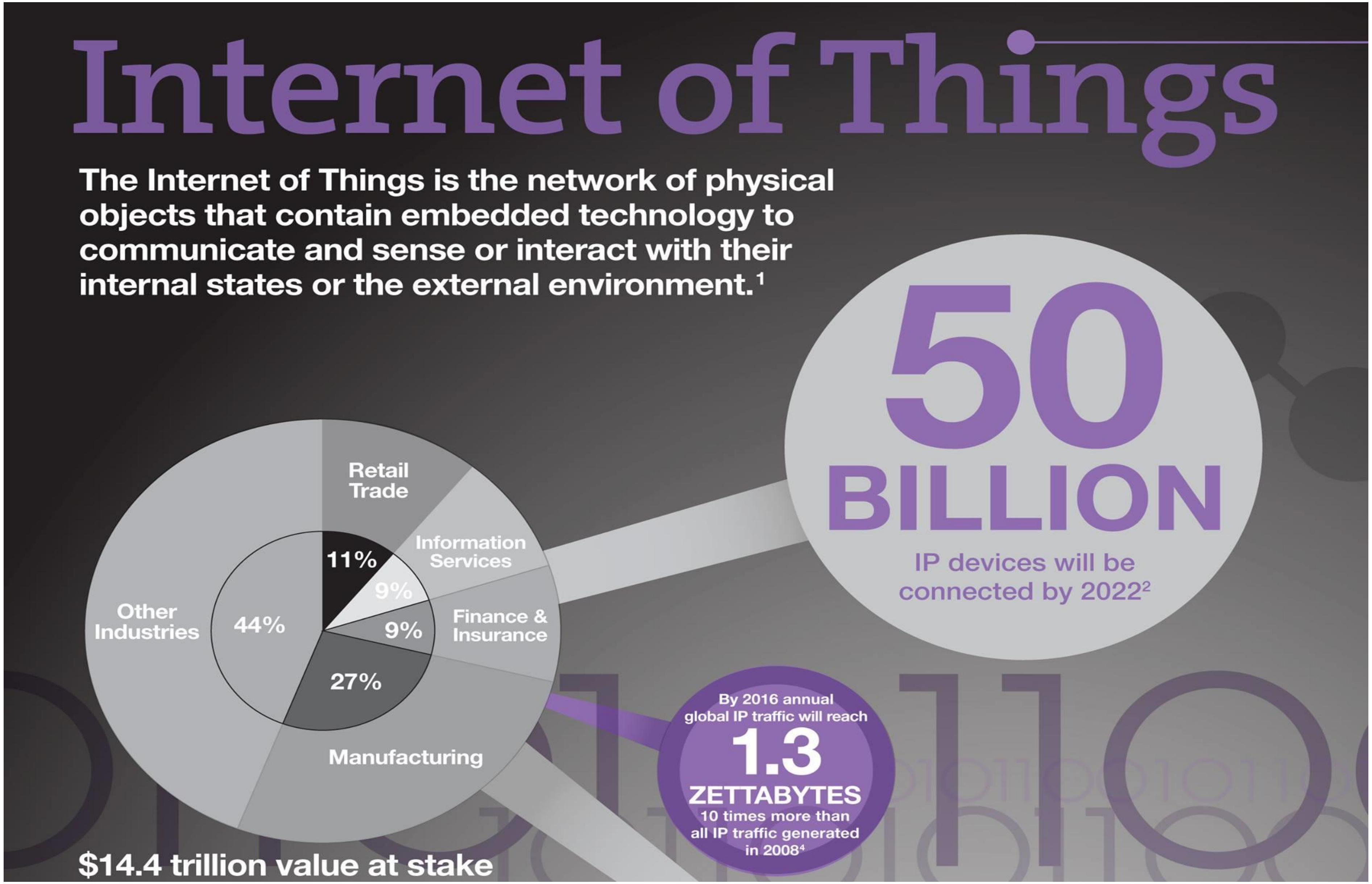
- Application whitelisting can help limit adversary initial infection vectors and should be used when not too invasive to the ICSs.
- DMZs and properly tuned firewalls between network segments will give visibility into the environment and allow defenders the time required to identify intrusions.
- Establish a central logging and data aggregation point to allow forensic evidence to be collected and made available to defenders.
- Implement alarm package priorities for abnormal cyber events within the control system.
- Enforce a password reset policy in the event of a compromise especially for VPNs and administrative accounts.
- Utilize up-to-date antivirus or endpoint security technologies to allow for the denial of known malware.
- Configure an intrusion detection system so that rules can be quickly deployed to search for intruders.

Architecture Recommendations: • Properly segment networks from each other. • Ensure logging is enabled on devices that support it, including both IT and Operational Technology (OT) assets. • Ensure that network architecture, such as switches, are managed and have the ability to capture data from the environment to support Passive and Active Defense mechanisms. • Make backups of critical software installers and include an MD5 and SHA256 digital hash of the installers. • Collect and vault backup project files from the network. • Test the tools and technologies that passive and active defense mechanisms will need (such as digital imaging software) on the environment to ensure that it will not negatively impact systems. • Prioritize and patch known vulnerabilities based on the most critical assets in the organization. • Limit remote connections only to personnel that need them. When personnel need remote access, ensure that if they do not need control that they do not have access to control elements. Use two-form authentication on the remote connections. • Consider use of a system event monitoring system, configured and monitored specifically for high-value ICS/SCADA systems.

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- Security and Privacy of Smart Cities
- References + Q&A

Internet of Things (IoT) Attack Surface



Internet of Things

The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.[1]

50 BILLION IP devices will be connected by 2022[2]

By 2016 annual global IP traffic will reach 1.3 ZETTABYTES 10 times more than all IP traffic generated in 2008[4]

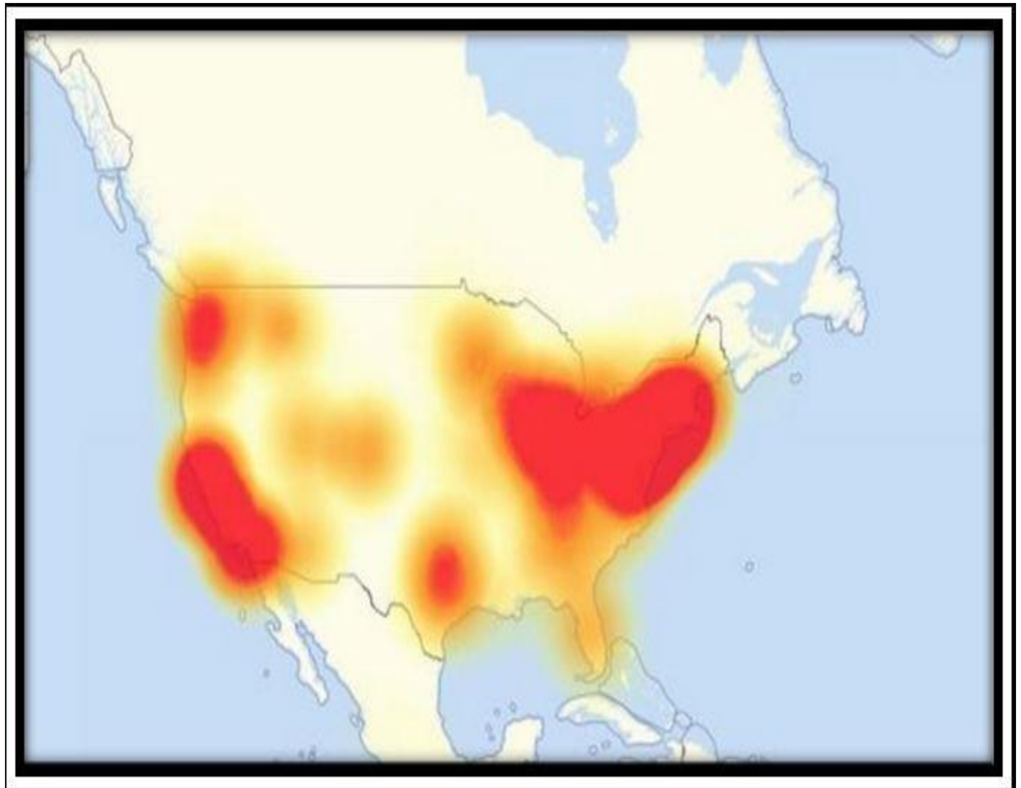
$14.4 trillion value at stake

Typical IoT Devices

CCTV cameras
DVRs
Digital TVs
Home routers
Printers
Alexa
Cars
Other stuff

Security systems
Garage doors
Industrial systems
Medical systems
Home appliances
Smart Utility Meters

Mirai Botnet: IoT Botnets Performed Massive Distributed Denial of Service Attacks (Oct 2016)



The Internet didn't "break" on October 21, 2016, but the attackers who launched the DDoS attacks against Dyn exploited a known DNS Weakness that negatively impacted MANY Internet-related businesses and millions of users.

What is Mirai Botnet

Mirai is a self-propagating botnet virus. The source code for Mirai was made publicly available by the author after a successful and well publicized attack on the Krebs Web site. Since then the source code has been built and used by many others to launch attacks on internet infrastructure (ref Dyn).

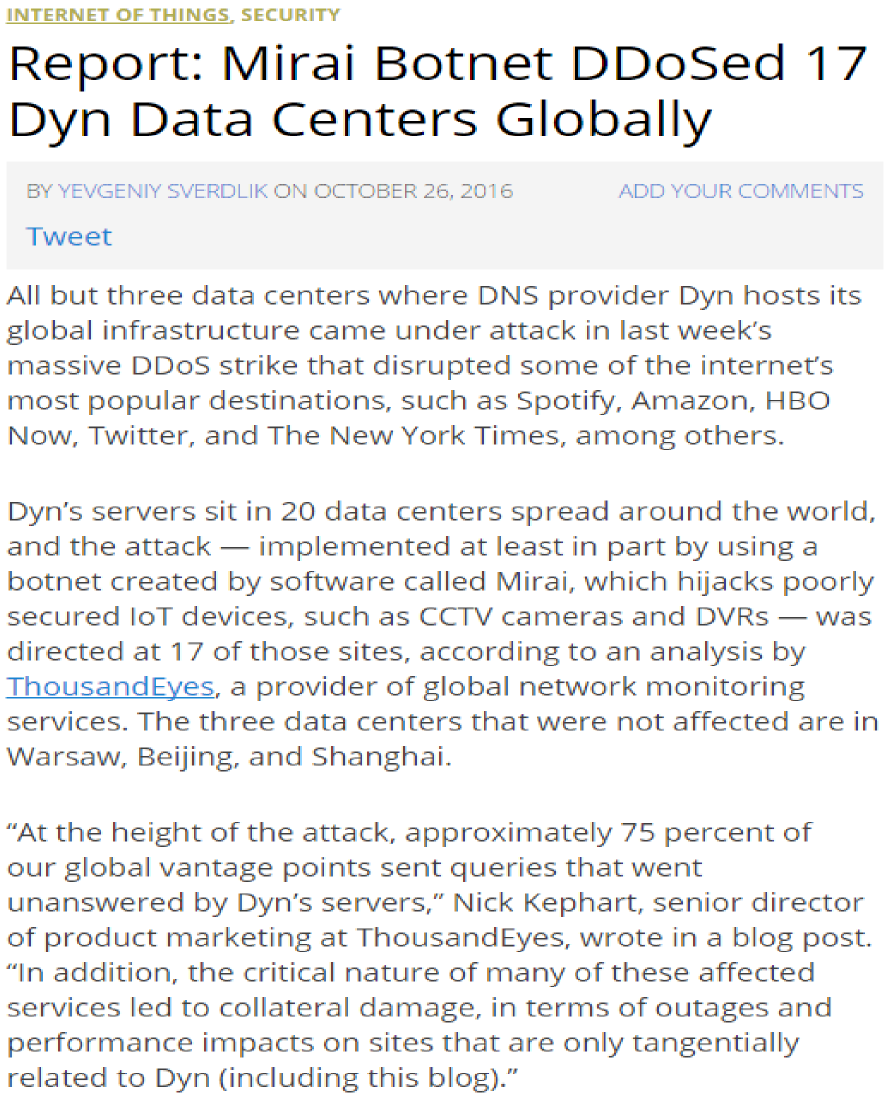
The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password. The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and co-ordinate them to mount a DDOS attack against a chosen victim.

http://www.billslater.com/mirai.ppsx

https://www.corero.com/resources/ddos-attack-types/mirai-botnet-ddos-attack.html

Mirai Impact

http://www.billslater.com/mirai.ppsx



INTERNET OF THINGS, SECURITY

Report: Mirai Botnet DDoSed 17 Dyn Data Centers Globally

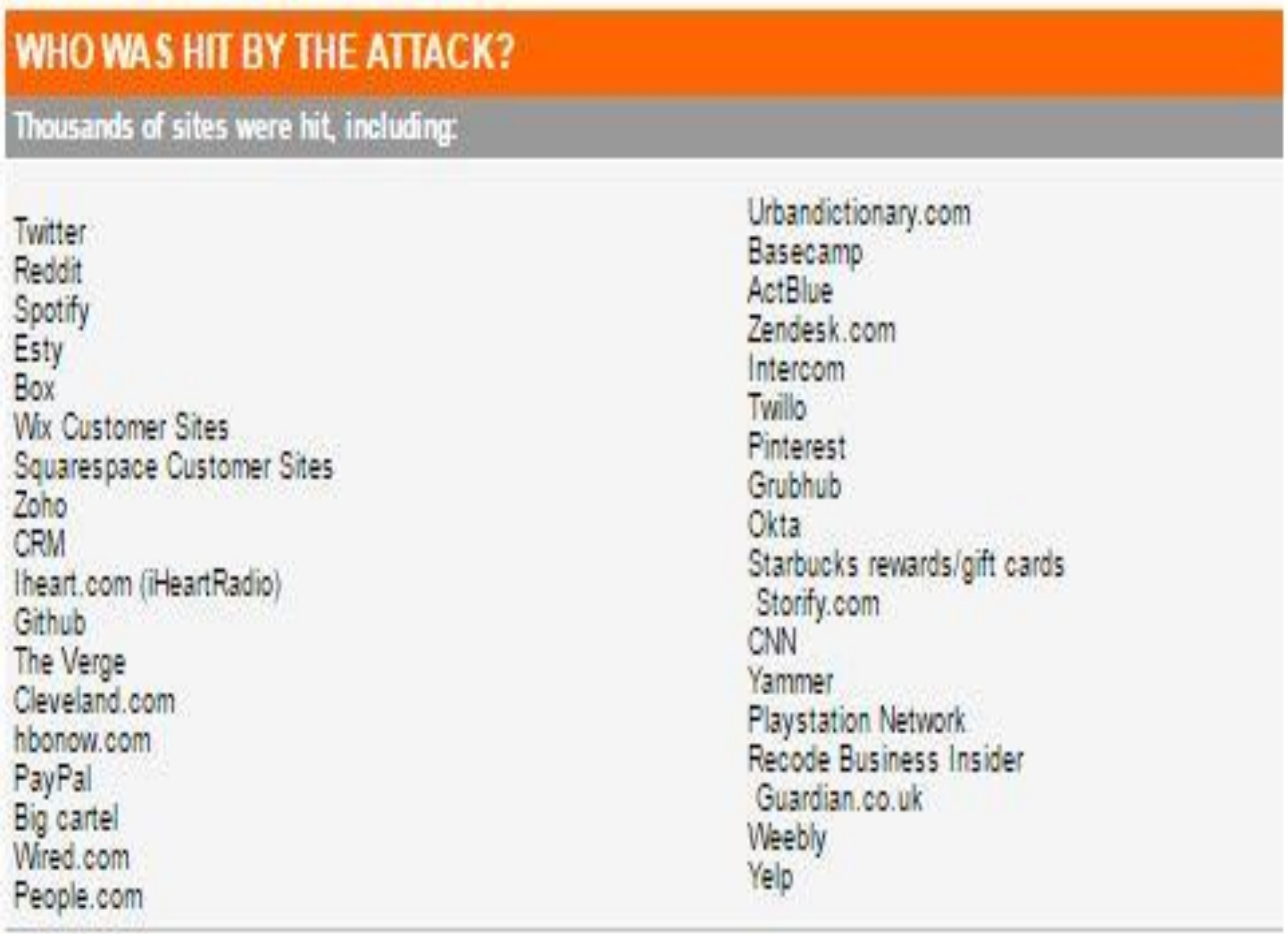
BY YEVGENIY SVERDLIK ON OCTOBER 26, 2016 ADD YOUR COMMENTS

Tweet

All but three data centers where DNS provider Dyn hosts its global infrastructure came under attack in last week's massive DDoS strike that disrupted some of the internet's most popular destinations, such as Spotify, Amazon, HBO Now, Twitter, and The New York Times, among others.

Dyn's servers sit in 20 data centers spread around the world, and the attack — implemented at least in part by using a botnet created by software called Mirai, which hijacks poorly secured IoT devices, such as CCTV cameras and DVRs — was directed at 17 of those sites, according to an analysis by ThousandEyes, a provider of global network monitoring services. The three data centers that were not affected are in Warsaw, Beijing, and Shanghai.

"At the height of the attack, approximately 75 percent of our global vantage points sent queries that went unanswered by Dyn's servers," Nick Kephart, senior director of product marketing at ThousandEyes, wrote in a blog post. "In addition, the critical nature of many of these affected services led to collateral damage, in terms of outages and performance impacts on sites that are only tangentially related to Dyn (including this blog)."



WHO WAS HIT BY THE ATTACK?

Thousands of sites were hit, including:

Twitter
Reddit
Spotify
Esty
Box
Wix Customer Sites
Squarespace Customer Sites
Zoho
CRM
Iheart.com (iHeartRadio)
Github
The Verge
Cleveland.com
hbonow.com
PayPal
Big cartel
Wired.com
People.com

Urbandictionary.com
Basecamp
ActBlue
Zendesk.com
Intercom
Twillo
Pinterest
Grubhub
Okta
Starbucks rewards/gift cards
Storify.com
CNN
Yammer
Playstation Network
Recode Business Insider
Guardian.co.uk
Weebly
Yelp

How Mirai Works (1 of 3)

http://www.billslater.com/mirai.ppsx

There are two main components to Mirai, the virus itself and the command and control center (CnC). The virus contains the attack vectors, Mirai has ten vectors that it can launch, and a scanner process that actively seeks other devices to compromise. The CnC is a separate image that controls the compromised devices (BOT) sending them instructions to launch one of the attacks against one or more victims.

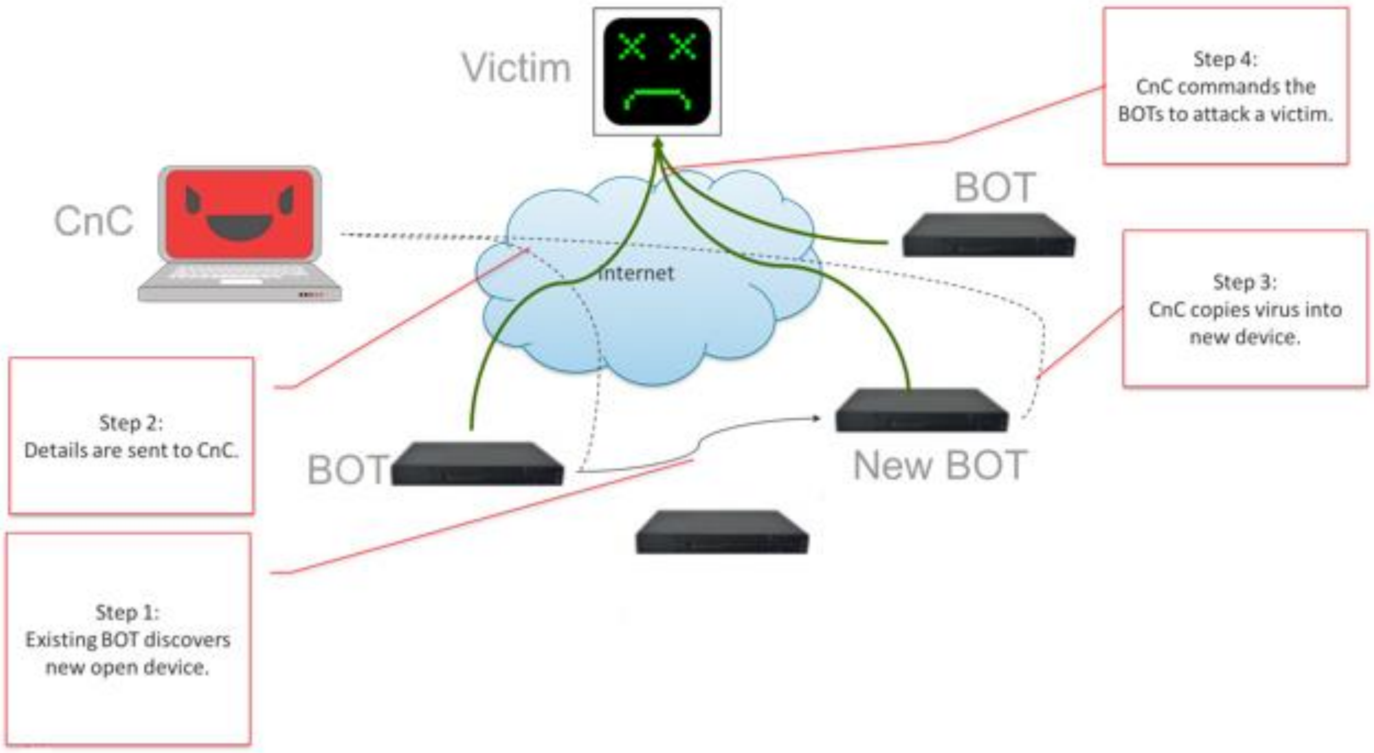

Victim
Step 4:
CnC commands the BOTs to attack a victim.
CnC
BOT
Internet
Step 3:
CnC copies virus into new device.
Step 2:
Details are sent to CnC.
BOT
New BOT
Step 1:
Existing BOT discovers new open device.

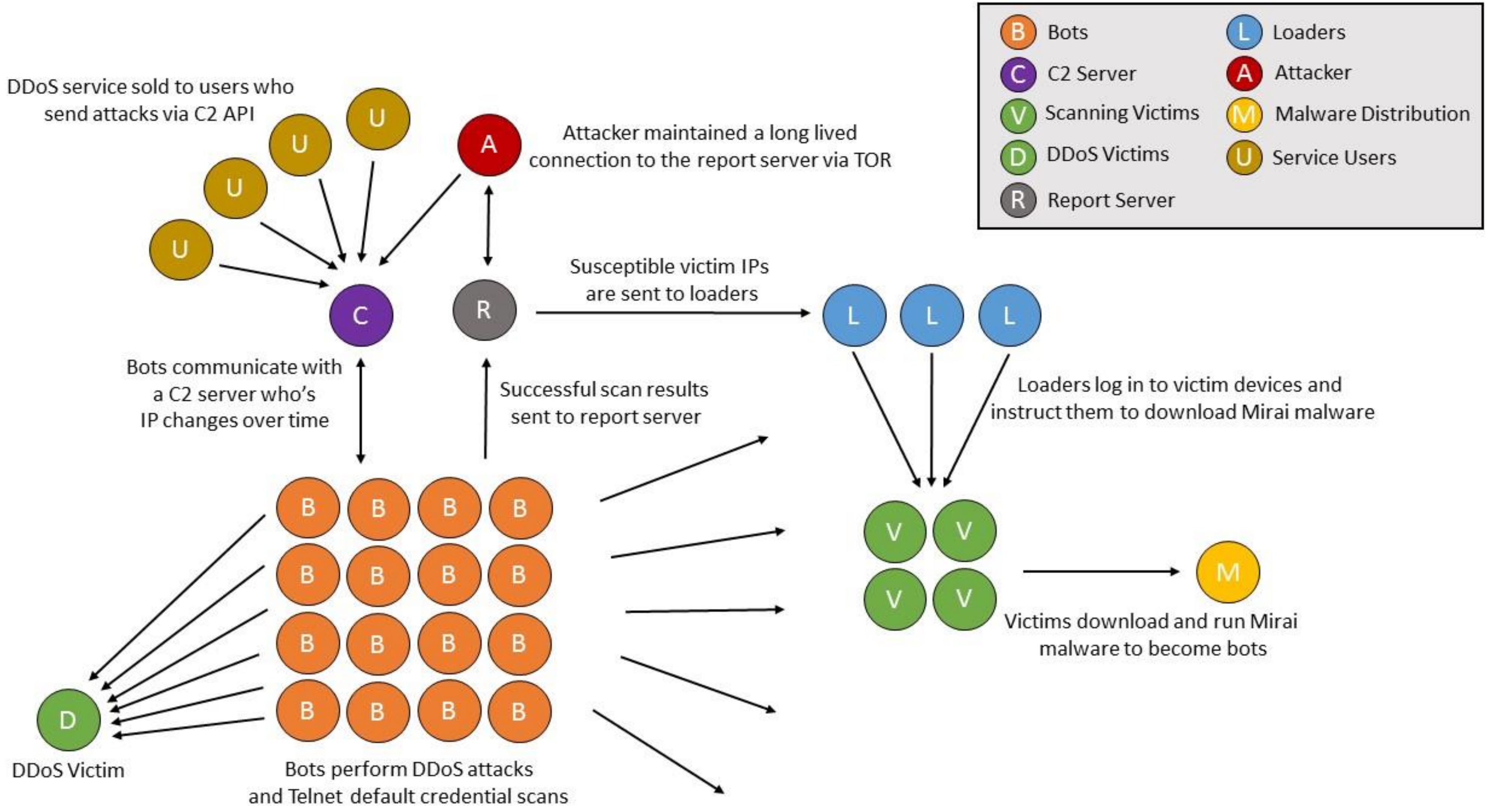
Figure 1 Mirai System

The scanner process runs continuously on each BOT using the telnet protocol (on TCP port 23 or 2323) to try and login to IP addresses at random. The login tries up to 60 different factory default username and password pairs when login succeeds the identity of the new BOT and its credentials are sent back to the CnC.

The CnC supports a simple command line interface that allows the attacker to specify an attack vector, a victim(s) IP address and an attack duration. The CnC also waits for its existing BOTs to return newly discovered device addresses and credentials which it uses to copy over the virus code and in turn create new BOTs.

How Mirai Works (2 of 3)

http://www.billslater.com/mirai.ppsx



B Bots

C C2 Server

V Scanning Victims

D DDoS Victims

R Report Server

L Loaders

A Attacker

M Malware Distribution

U Service Users

DDoS service sold to users who send attacks via C2 API

Attacker maintained a long lived connection to the report server via TOR

Susceptible victim IPs are sent to loaders

Bots communicate with a C2 server who's IP changes over time

Successful scan results sent to report server

Loaders log in to victim devices and instruct them to download Mirai malware

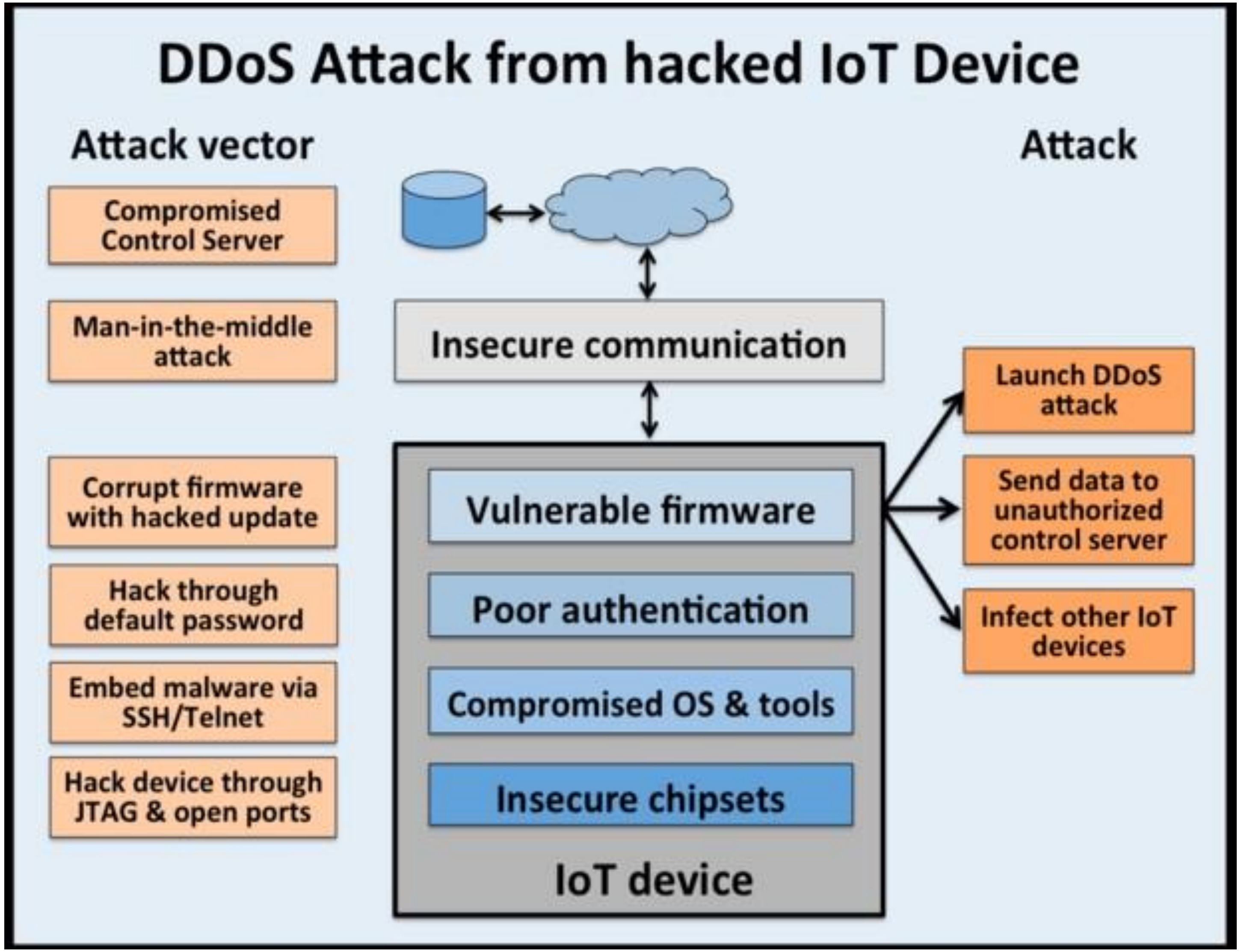
Victims download and run Mirai malware to become bots

DDoS Victim

Bots perform DDoS attacks and Telnet default credential scans

How Mirai Works (3 of 3)

http://www.billslater.com/mirai.ppsx


DDoS Attack from hacked IoT Device
Attack vector
Attack
Compromised Control Server
Man-in-the-middle attack
Corrupt firmware with hacked update
Hack through default password
Embed malware via SSH/Telnet
Hack device through JTAG & open ports
Insecure communication
Vulnerable firmware
Poor authentication
Compromised OS & tools
Insecure chipsets
IoT device
Launch DDoS attack
Send data to unauthorized control server
Infect other IoT devices

Infected IoT Devices:

1) Launch DDoS Attacks
2) Report data to C2 Servers
3) Infect other IoT Devices

9/24/2019

Where Mirai Botnet Attacks Came From

http://www.billslater.com/mirai.ppsx

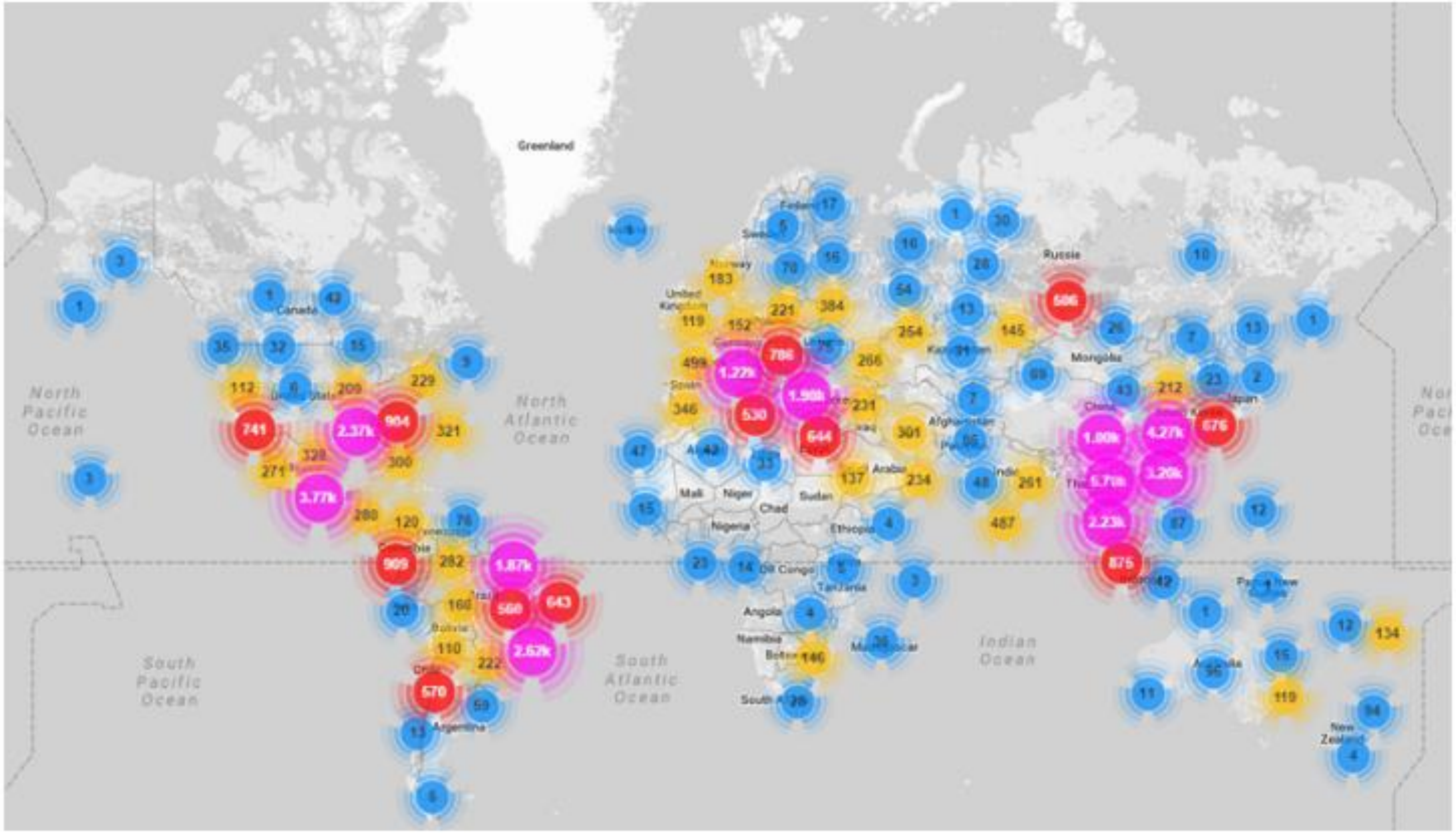


Figure 2: Geo-locations of all Mirai-infected devices uncovered so far

Country	% of Mirai botnet IPs
Vietnam	12.8%
Brazil	11.8%
United States	10.9%
China	8.8%
Mexico	8.4%
South Korea	6.2%
Taiwan	4.9%
Russia	4.0%
Romania	2.3%
Colombia	1.5%

Source:
https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

Mirai – Statistical View of the Attacks

- Mirai-powered GRE floods, peaked at 280 Gbps/130 Mpps
- Investigation of the attack uncovered 49,657 unique IPs which hosted Mirai-infected devices. As previously reported, these were mostly CCTV cameras—a popular choice of DDoS botnet herders.
- Other victimized devices included DVRs and routers.
- Overall, IP addresses of Mirai-infected devices were spotted in 164 countries. As evidenced by the map below, the botnet IPs are highly dispersed, appearing even in such remote locations as Montenegro, Tajikistan and Somalia.

Protecting IoT Devices Against Mirai (Botnets)

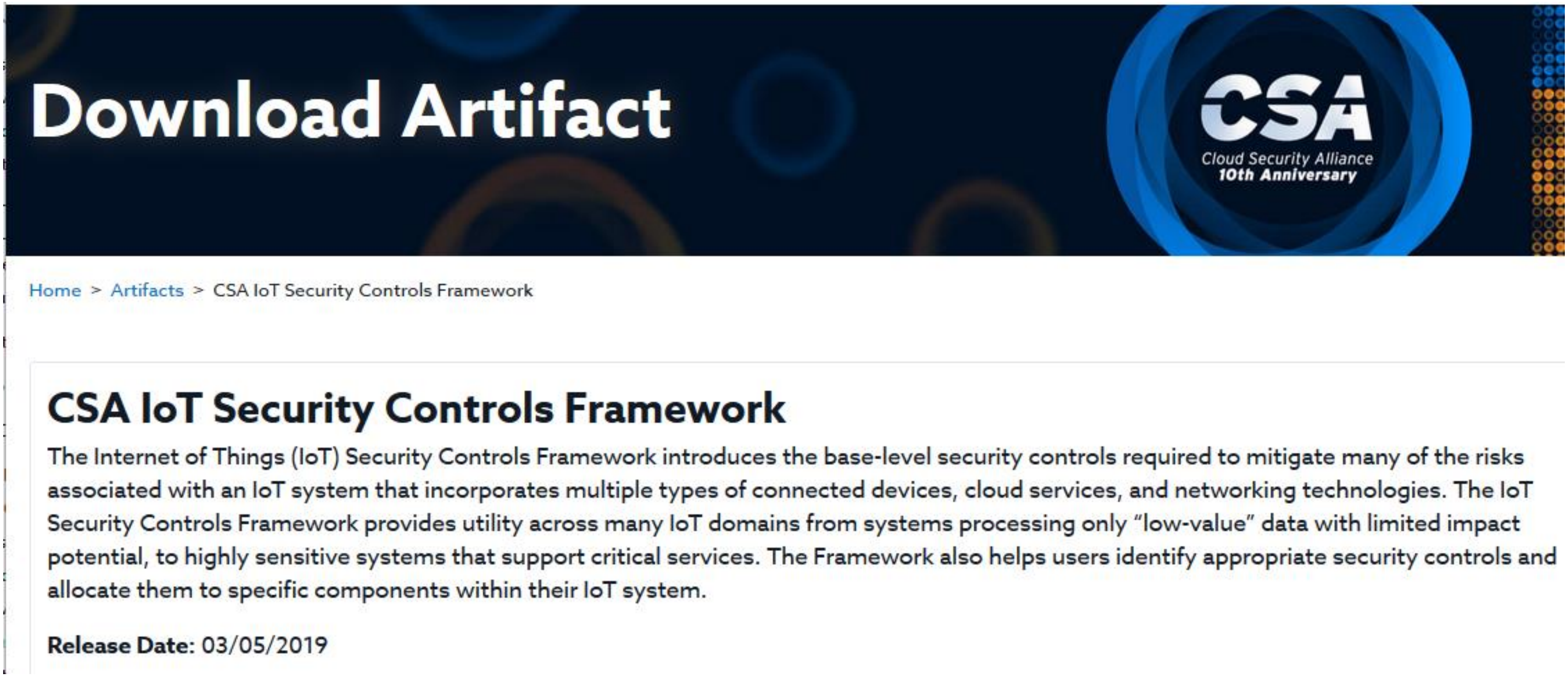
http://www.billslater.com/mirai.ppsx

- ***Change Your Password.*** This is not only good advice for those of us who shop online or who have been notified that the e-commerce site we recently shopped on has been breached, but likewise for IoT devices. In fact, according to this report, these better credentials can be used to provide a bulwark against botnet attacks like Mirai by substituting the hard-coded username and password with ones that are unique to your organization and not, of course, easily guessed.
- ***Turn them off.*** For currently deployed IoT devices, turn them off when not in use. If the Mirai botnet does infect a device, the password must be reset and the system rebooted to get rid of it.
- ***Disable all remote access to them.*** To protect devices from Mirai and other botnets, users should not only shield TCP/23 and TCP/2323 access to those devices, but also to disable all remote (WAN) access to them.
- ***Research Your Purchase.*** Before you even buy a product, research what you are buying and make sure that you know how to update any software associated with the device. Look for devices, systems, and services that make it easy to update the device and inform the end user when updates are available.
- ***Use It or Lose It.*** Once the product is in your office, turn off the functions you're are not using. Enabled functionality usually comes with increased security risks. Again, make sure you review that before you even bring the product into the workplace. If it's already there, don't be shy about calling customer service and walking through the steps needed to shut down any unused functions.

Source:
https://www.pwnieexpress.com/blog/mirai-botnet-part-2

Cloud Security Alliance (CSA) Internet of Things (IoT) Security Controls Framework

https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/



Home > Artifacts > CSA IoT Security Controls Framework

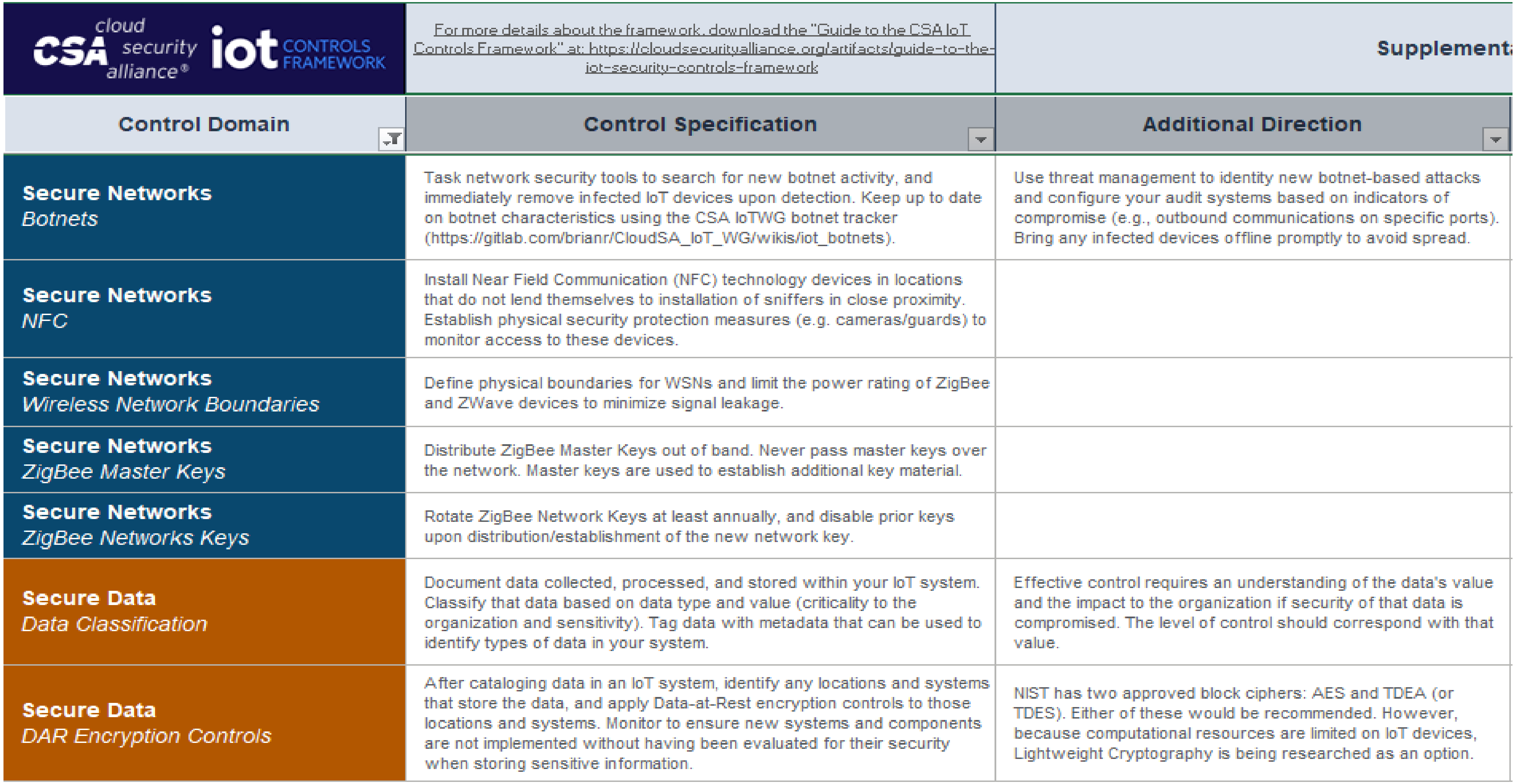
CSA IoT Security Controls Framework

The Internet of Things (IoT) Security Controls Framework introduces the base-level security controls required to mitigate many of the risks associated with an IoT system that incorporates multiple types of connected devices, cloud services, and networking technologies. The IoT Security Controls Framework provides utility across many IoT domains from systems processing only "low-value" data with limited impact potential, to highly sensitive systems that support critical services. The Framework also helps users identify appropriate security controls and allocate them to specific components within their IoT system.

Release Date: 03/05/2019

Cloud Security Alliance (CSA) Internet of Things (IoT) Security Controls Framework

https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/


cloud security alliance® CSA
iot CONTROLS FRAMEWORK

	For more details about the framework, download the "Guide to the CSA IoT Controls Framework" at: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework	Supplement
Control Domain	**Control Specification**	**Additional Direction**
Secure Networks *Botnets*	Task network security tools to search for new botnet activity, and immediately remove infected IoT devices upon detection. Keep up to date on botnet characteristics using the CSA IoTWG botnet tracker (https://gitlab.com/brianr/CloudSA_IoT_WG/wikis/iot_botnets).	Use threat management to identity new botnet-based attacks and configure your audit systems based on indicators of compromise (e.g., outbound communications on specific ports). Bring any infected devices offline promptly to avoid spread.
Secure Networks *NFC*	Install Near Field Communication (NFC) technology devices in locations that do not lend themselves to installation of sniffers in close proximity. Establish physical security protection measures (e.g. cameras/guards) to monitor access to these devices.	
Secure Networks *Wireless Network Boundaries*	Define physical boundaries for WSNs and limit the power rating of ZigBee and ZWave devices to minimize signal leakage.	
Secure Networks *ZigBee Master Keys*	Distribute ZigBee Master Keys out of band. Never pass master keys over the network. Master keys are used to establish additional key material.	
Secure Networks *ZigBee Networks Keys*	Rotate ZigBee Network Keys at least annually, and disable prior keys upon distribution/establishment of the new network key.	
Secure Data *Data Classification*	Document data collected, processed, and stored within your IoT system. Classify that data based on data type and value (criticality to the organization and sensitivity). Tag data with metadata that can be used to identify types of data in your system.	Effective control requires an understanding of the data's value and the impact to the organization if security of that data is compromised. The level of control should correspond with that value.
Secure Data *DAR Encryption Controls*	After cataloging data in an IoT system, identify any locations and systems that store the data, and apply Data-at-Rest encryption controls to those locations and systems. Monitor to ensure new systems and components are not implemented without having been evaluated for their security when storing sensitive information.	NIST has two approved block ciphers: AES and TDEA (or TDES). Either of these would be recommended. However, because computational resources are limited on IoT devices, Lightweight Cryptography is being researched as an option.

Table of Contents

- Introduction – IT Pro SI on Cyberthreats and Security
- Grid Cybersecurity (Ukraine)
- CSA IoT Security (Controls and Mitigations)
- Security and Privacy of Smart Cities
- References + Q&A

References Used in This Presentation

- Scoping the Cyber Security Body of Knowledge” Awais Rashid et al, IEEE Security and PrivacyMagazine, Volume 16, Issue 3, May, June 2018

- E-ISAC, SANS ICS. “Analysis of the Cyber Attack on the Ukrainian Power Grid” March 18 2016. p4. http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

- Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks- https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

- THREAT INTELLIGENCE REPORT CYBERATTACKS AGAINST UKRAINIAN ICS https://www.sentryo.net/wp-content/uploads/2017/09/EBOOK_CYBERATTACKS-AGAINST-UKRAINIAN-ICS.pdf

- Kapersky Black Energy Spearphishing Attack Agains Ukraine ICS https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents

- A Nation Under Attack: Advanced Cyber-Attacks in Ukraine (YoutTube – 2018 https://www.youtube.com/watch?v=HgDbpTiTFdw

IoT Security References Used in the CSA Guidleines

- Data Processing Stream; Fujitsu Laboratories Ltd., Kawasaki, Japan, March 7, 2018. http://www.fujitsu.com/global/about/resources/news/press-releases/2018/0307-02.html

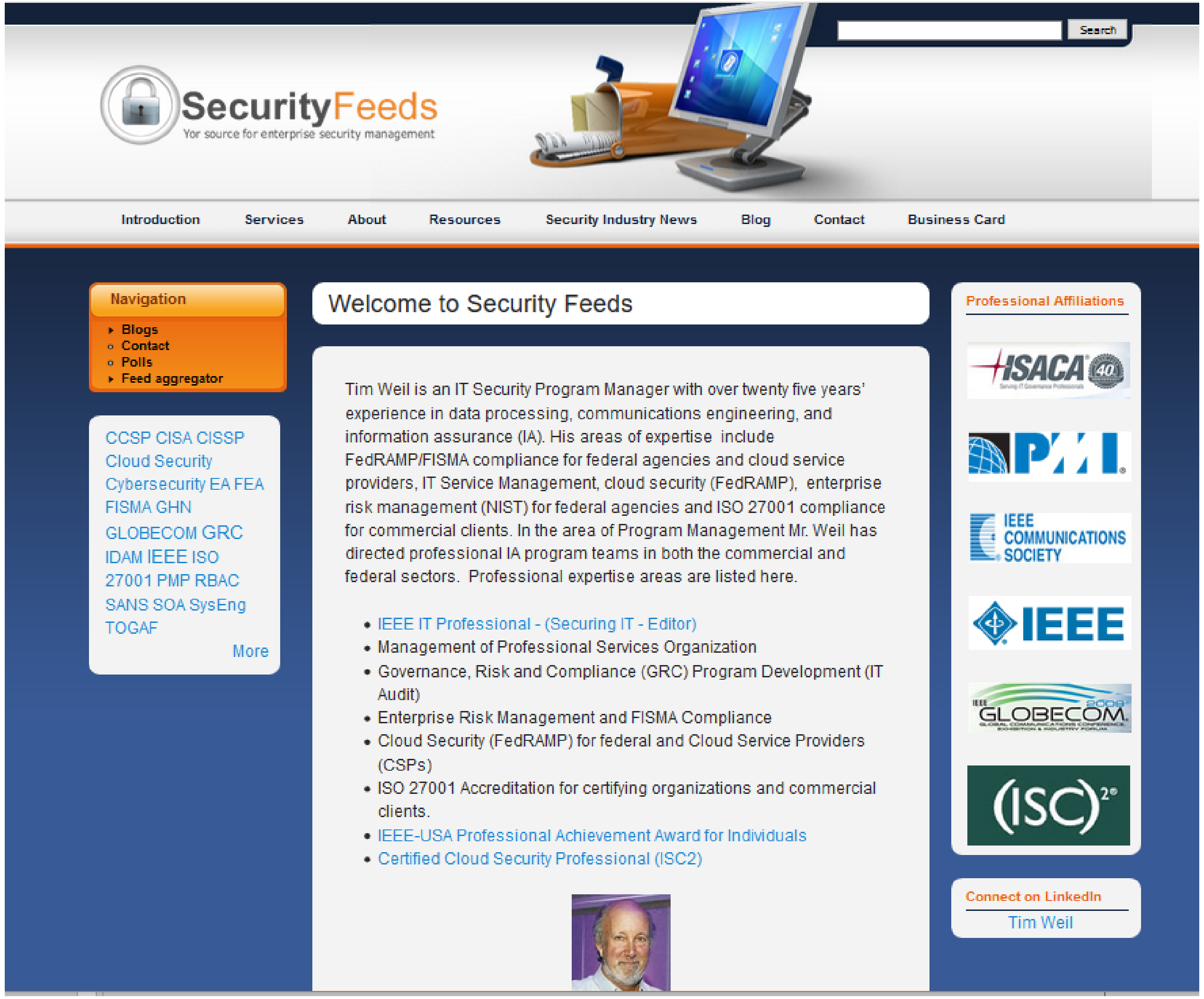
- Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT), Draft NISTIR 8200; National Institute of Standards and Technology; February 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200- draft.pdf

- “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” European Union Agency for Network and Information Security (ENISA); November 20, 2017. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

- “Internet of Things--Reference Architecture,” ISO/IEC JTC 1/SC 41; August 2018. https://www.iso.org/standard/65695.html

Thank you for joining us!

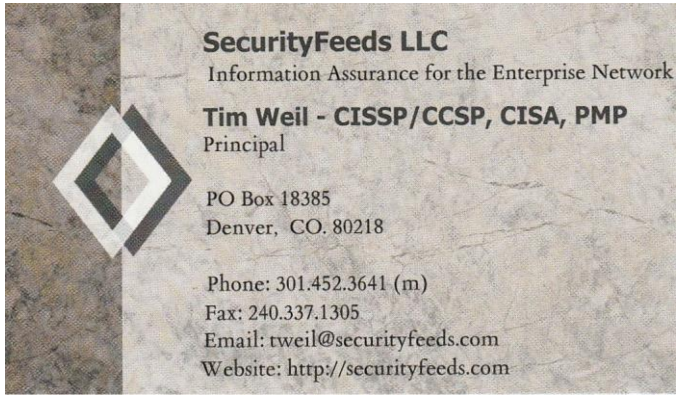
SecurityFeeds Website - http://securityfeeds.com/



Welcome to Security Feeds

Tim Weil is an IT Security Program Manager with over twenty five years' experience in data processing, communications engineering, and information assurance (IA). His areas of expertise include FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security (FedRAMP), enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients. In the area of Program Management Mr. Weil has directed professional IA program teams in both the commercial and federal sectors. Professional expertise areas are listed here.

- IEEE IT Professional - (Securing IT - Editor)
- Management of Professional Services Organization
- Governance, Risk and Compliance (GRC) Program Development (IT Audit)
- Enterprise Risk Management and FISMA Compliance
- Cloud Security (FedRAMP) for federal and Cloud Service Providers (CSPs)
- ISO 27001 Accreditation for certifying organizations and commercial clients.
- IEEE-USA Professional Achievement Award for Individuals
- Certified Cloud Security Professional (ISC2)

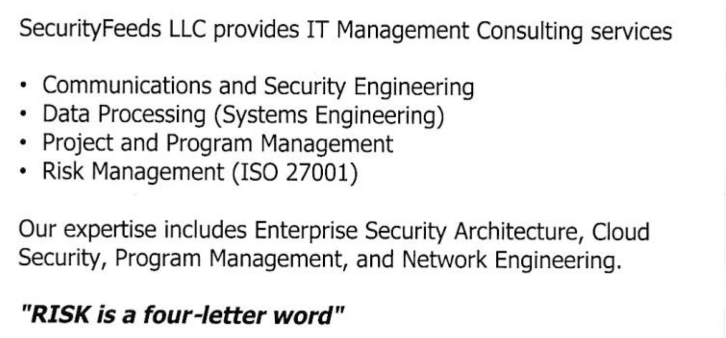


SecurityFeeds LLC
Information Assurance for the Enterprise Network

Tim Weil - CISSP/CCSP, CISA, PMP
Principal

PO Box 18385
Denver, CO. 80218

Phone: 301.452.3641 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com



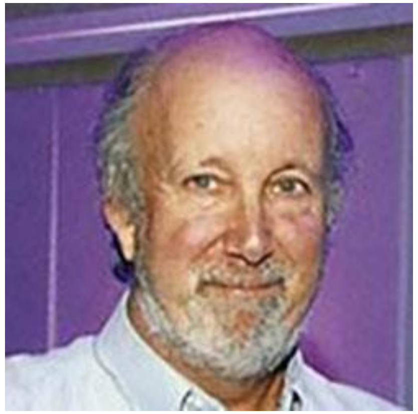
SecurityFeeds LLC provides IT Management Consulting services

- Communications and Security Engineering
- Data Processing (Systems Engineering)
- Project and Program Management
- Risk Management (ISO 27001)

Our expertise includes Enterprise Security Architecture, Cloud Security, Program Management, and Network Engineering.

"RISK is a four-letter word"

Tim Weil – Network Program Manager



Tim is a Security Architect/IT Security Manager with over twenty five years of IT management, consulting and engineering experience in the U.S. Government and Communications Industry. His technical areas of expertise includes FedRAMP/FISMA compliance for federal agencies and cloud service providers, IT Service Management, cloud security, enterprise risk management (NIST) for federal agencies and ISO 27001 compliance for commercial clients.

He is a Senior Member of the IEEE and has served in several IEEE positions -

Chair of the Denver Section (2013); Chair of the Washington Section (2009); Cybersecurity Editor for IEEE IT Professional magazine. General Chair - IEEE GREENTECH Conference (2013)

His publications, blogs and speaking engagements are available from the website - http://securityfeeds.com

SCRAM SYSTEMS